



US009300910B2

(12) **United States Patent**
Shoemake et al.

(10) **Patent No.:** **US 9,300,910 B2**
(45) **Date of Patent:** **Mar. 29, 2016**

(54) **VIDEO MAIL CAPTURE, PROCESSING AND DISTRIBUTION**

(71) Applicant: **Biscotti Inc.**, McKinney, TX (US)

(72) Inventors: **Matthew B. Shoemake**, Allen, TX (US);
Syed Nadeem Ahmed, Allen, TX (US);
Craig D. Smith, Allen, TX (US); **Jack R. Ring**, Lewisville, TX (US)

(73) Assignee: **Biscotti Inc.**, Plano, TX (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **14/170,499**

(22) Filed: **Jan. 31, 2014**

(65) **Prior Publication Data**

US 2014/0168344 A1 Jun. 19, 2014

Related U.S. Application Data

(63) Continuation-in-part of application No. 14/106,263, filed on Dec. 13, 2013, and a continuation-in-part of application No. 14/106,279, filed on Dec. 13, 2013, and a continuation-in-part of application No.

(Continued)

(51) **Int. Cl.**
H04N 7/16 (2011.01)
H04N 7/14 (2006.01)
(Continued)

(52) **U.S. Cl.**
CPC **H04N 7/147** (2013.01); **H04M 3/5315** (2013.01); **H04M 1/6505** (2013.01); **H04M 1/72555** (2013.01)

(58) **Field of Classification Search**
USPC 348/14.01
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,058,307 A 5/2000 Garner
6,614,465 B2 9/2003 Alexander et al.

(Continued)

FOREIGN PATENT DOCUMENTS

EP 1814290 A2 8/2007
JP 2010/152866 A 7/2010

(Continued)

OTHER PUBLICATIONS

Amazon "Amazon Cloud Front Documentation" 3 pages, Available at: <http://aws.amazon.com/documentation/cloudfront/>; Accessed on Feb. 25, 2014.

(Continued)

Primary Examiner — James Hannett

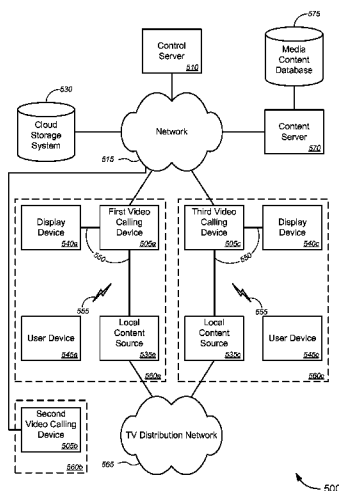
Assistant Examiner — Stephen Coleman

(74) *Attorney, Agent, or Firm* — Swanson & Bratschun, L.L.C.

(57) **ABSTRACT**

Novel tools and techniques are provided for enabling or implementing video mail capture, processing, and distribution. In response to a first video calling device receiving a video call from a caller at a second video calling device, the first video calling device, which is associated with a user or callee, might determine whether the user is available to answer the video call. If not, one of the first or second video calling devices might prompt the caller to leave a videomail message, and might record and upload the videomail message to a server over a network for post-processing and/or storage. A notification may be sent to the user regarding the videomail message. The user may be provided with options to view the videomail message and/or to respond to the videomail message. In some cases, the first and second video calling devices might be of different make or model.

25 Claims, 8 Drawing Sheets



Related U.S. Application Data

- 14/106,360, filed on Dec. 13, 2013, now Pat. No. 8,914,837.
- (60) Provisional application No. 61/877,928, filed on Sep. 13, 2013, provisional application No. 61/874,903, filed on Sep. 6, 2013, provisional application No. 61/872,603, filed on Aug. 30, 2013, provisional application No. 61/858,518, filed on Jul. 25, 2013, provisional application No. 61/759,621, filed on Feb. 1, 2013, provisional application No. 61/737,506, filed on Dec. 14, 2012.
- (51) **Int. Cl.**
H04M 3/53 (2006.01)
H04M 1/725 (2006.01)
H04M 1/65 (2006.01)

(56) References Cited

U.S. PATENT DOCUMENTS

- 6,638,113 B2 10/2003 Kajiwara et al.
 6,804,224 B1 10/2004 Schuster et al.
 7,039,393 B1* 5/2006 Kite 455/412.2
 7,084,904 B2 8/2006 Liu et al.
 7,587,289 B1 9/2009 Sivertsen
 7,646,404 B2 1/2010 Liu et al.
 7,768,388 B2 8/2010 Putterman et al.
 8,063,929 B2 11/2011 Kurtz et al.
 8,122,491 B2 2/2012 Yee et al.
 8,144,182 B2 3/2012 Shoemake et al.
 8,239,903 B1 8/2012 Campagna et al.
 8,300,082 B2 10/2012 Malik
 8,325,213 B2 12/2012 Lamb et al.
 8,330,795 B2 12/2012 Iyer et al.
 8,366,487 B2 2/2013 Weng et al.
 8,395,652 B1 3/2013 Chapweske et al.
 8,566,838 B2 10/2013 Sabin et al.
 8,914,837 B2 12/2014 Ahmed et al.
 9,253,520 B2 2/2016 Shoemake et al.
 2001/0001159 A1 5/2001 Ford
 2001/0032246 A1 10/2001 Fardella et al.
 2002/0059094 A1 5/2002 Hosea et al.
 2002/0073420 A1 6/2002 Yoon
 2002/0118675 A1 8/2002 Strathmeyer et al.
 2003/0160871 A1 8/2003 Pelletier et al.
 2003/0200105 A1* 10/2003 Borden et al. 705/1
 2004/0027624 A1 2/2004 Parulski et al.
 2004/0061787 A1 4/2004 Liu et al.
 2004/0114919 A1 6/2004 Rife
 2004/0145658 A1 7/2004 Lev-Ran et al.
 2005/0007445 A1 1/2005 Foote et al.
 2005/0066357 A1 3/2005 Ryal
 2005/0086069 A1 4/2005 Watson et al.
 2005/0095084 A1* 5/2005 Hansen 411/508
 2005/0195954 A1 9/2005 Klein et al.
 2005/0246738 A1 11/2005 Lockett et al.
 2005/0283813 A1* 12/2005 Jamail et al. 725/109
 2006/0031291 A1 2/2006 Beckemeyer
 2006/0107281 A1 5/2006 Dunton
 2006/0110136 A1 5/2006 Abecassis
 2006/0130118 A1 6/2006 Damm
 2006/0130119 A1 6/2006 Candelore et al.
 2006/0187306 A1 8/2006 Matsui
 2006/0209194 A1 9/2006 Liu et al.
 2006/0268149 A1* 11/2006 Teng 348/362
 2007/0067407 A1* 3/2007 Bettis et al. 709/207
 2007/0161386 A1 7/2007 Faber et al.
 2007/0188597 A1 8/2007 Kenoyer
 2007/0203708 A1 8/2007 Polcyn et al.
 2007/0204288 A1 8/2007 Candelore
 2007/0239825 A1 10/2007 Walter
 2007/0271580 A1 11/2007 Tischer et al.
 2008/0028318 A1* 1/2008 Shikuma 715/744

- 2008/0040380 A1 2/2008 Miyaki
 2008/0062253 A1 3/2008 Jaspersohn et al.
 2008/0152096 A1 6/2008 Archer
 2008/0189617 A1 8/2008 Covell et al.
 2008/0201369 A1 8/2008 Cordoba
 2008/0222673 A1 9/2008 Durden et al.
 2008/0270589 A1 10/2008 Hwang
 2008/0292139 A1* 11/2008 Wadhwa et al. 382/100
 2008/0307105 A1* 12/2008 Sethi et al. 709/231
 2009/0037945 A1 2/2009 Greig et al.
 2009/0232129 A1 9/2009 Wong et al.
 2009/0281897 A1 11/2009 Antos
 2010/0060477 A1 3/2010 Laasik et al.
 2010/0064334 A1 3/2010 Blackburn et al.
 2010/0131363 A1 5/2010 Sievert et al.
 2010/0157013 A1 6/2010 Sylvain
 2010/0169410 A1 7/2010 Lund et al.
 2010/0218170 A1 8/2010 MacLellan et al.
 2010/0220188 A1 9/2010 Renkis
 2010/0232758 A1 9/2010 Cook et al.
 2010/0266111 A1 10/2010 Crausaz et al.
 2010/0306379 A1 12/2010 Ferris
 2011/0029370 A1 2/2011 Roeding et al.
 2011/0035271 A1 2/2011 Weaver et al.
 2011/0069179 A1 3/2011 Bathiche et al.
 2011/0075011 A1 3/2011 Abebe
 2011/0193971 A1 8/2011 Lin
 2011/0205329 A1 8/2011 Willis
 2011/0211678 A1 9/2011 Woodworth et al.
 2011/0254914 A1 10/2011 Ng
 2011/0317587 A1 12/2011 Lida et al.
 2012/0002849 A1 1/2012 Tokuse
 2012/0019609 A1 1/2012 Chang et al.
 2012/0054809 A1 3/2012 Chowdhury et al.
 2012/0072936 A1 3/2012 Small et al.
 2012/0081501 A1 4/2012 Benzaia et al.
 2012/0081502 A1 4/2012 Naidu et al.
 2012/0102533 A1 4/2012 Park
 2012/0133515 A1 5/2012 Palshof
 2012/0166517 A1 6/2012 Lee et al.
 2012/0189282 A1* 7/2012 Wyatt et al. 386/278
 2012/0203823 A1 8/2012 Manglik et al.
 2012/0206553 A1 8/2012 MacDonald
 2012/0207088 A1 8/2012 Liu et al.
 2012/0226752 A1 9/2012 Jeong et al.
 2012/0229591 A1 9/2012 Lee
 2012/0236127 A1 9/2012 Ojala et al.
 2012/0266252 A1 10/2012 Spiers et al.
 2012/0315793 A1 12/2012 Hermann et al.
 2012/0331113 A1 12/2012 Jain et al.
 2013/0007157 A1 1/2013 Eftis et al.
 2013/0046280 A1 2/2013 Martin et al.
 2013/0083150 A1 4/2013 Howarter et al.
 2013/0174194 A1 7/2013 Mooneyham
 2013/0231183 A1 9/2013 Zalewski
 2013/0265384 A1 10/2013 Shoemake et al.
 2013/0344961 A1 12/2013 Iannetta
 2014/0123162 A1 5/2014 Karlsson et al.
 2014/0168071 A1 6/2014 Ahmed et al.
 2014/0168453 A1 6/2014 Shoemake et al.
 2014/0173675 A1 6/2014 Ahmed et al.
 2014/0333713 A1 11/2014 Shoemake et al.
 2014/0359647 A1 12/2014 Shoemake et al.
 2014/0375752 A1 12/2014 Shoemake et al.
 2015/0026708 A1 1/2015 Ahmed et al.
 2015/0070516 A1 3/2015 Shoemake et al.
 2015/0243163 A1 8/2015 Shoemake
 2015/0244807 A1 8/2015 Shoemake et al.
 2015/0324076 A1 11/2015 Ahmed et al.
 2015/0334344 A1 11/2015 Shoemake et al.

FOREIGN PATENT DOCUMENTS

- KR 2010/0062559 A 6/2010
 KR 2012/0139251 A 12/2012
 WO WO 2010/118202 A1 10/2010
 WO WO 2010/147281 A1 12/2010
 WO WO 2012/076724 A1 6/2012
 WO WO 2014/093931 A1 6/2014

(56)

References Cited**FOREIGN PATENT DOCUMENTS**

WO	WO 2014/093932	A1	6/2014
WO	WO 2014/093933	A1	6/2014
WO	WO 2014/121148	A1	8/2014
WO	WO 2015/013592	A1	1/2015
WO	WO 2015/031671	A1	3/2015
WO	WO 2015/035247	A1	3/2015

OTHER PUBLICATIONS

AWS, Amazon Elastic Compute Cloud (EC2), Amazon Web Services LLC, 6 pages, Available at: <http://aws.amazon.com/ec2/>; Accessed on Mar. 3, 2014.

AWS, Amazon Simple Storage Service, Amazon Web Services, Inc., 6 pages, Available at: <http://aws.amazon.com/s3/>; Accessed on Mar. 3, 2014.

Amazon "Amazon Simple Storage Service Getting Started Guide" Mar. 1, 2006, 20 pages, Amazon Web Services LLC.

Anderson "SETI@home: An Experiment in Public-Resource Computing" (Nov. 2002) 8 pages, Space Sciences Laboratory, U.C. Berkeley.

Apple "Apple TV 3rd Generation Setup Guide" 36 pages.

Apple, "iOS 8 FaceTime" video calling service; Available at: <http://www.apple.com/ios/facetime/>; Accessed on Oct. 2, 2014; 3 pages.

Apple "iPhoto for Mac" 6 pages, Available at: <https://www.apple.com/mac/iphoto/>; Accessed on Feb. 28, 2014.

Apple "OS X Mavericks, Mac App Store" 5 pages, Available at: <http://www.apple.com/osx/apps/app-store.html>; Accessed on Feb. 28, 2014.

Biscotti camera products; Available at: <http://biscotti.com/biscotti>; Accessed on Oct. 2, 2014; 1 page.

Blue Host, "The Best Web Hosting", Available at: <http://www.bluehost.com/>; Accessed on Oct. 2, 2014; 3 pages.

BlueJeans Network; Multi-Party Conferencing in the Cloud; Available at: <http://www.bluejeans.com>; Accessed on Oct. 2, 2014; 3 pages.

Cerf et al. (1974) "Specification of Internet Transmission Control Program" Network Working Group; 70 pages.

Cisco Collaboration Endpoints; Video calling cameras and systems; Available at: <http://www.cisco.com/c/en/us/products/collaboration-endpoints/product-listing.html>. Accessed on Oct. 2, 2014; 2 pages.

Data Center Virtualization and Cloud Infrastructure Products; Available at: <http://www.vmware.com/products/datacenter-virtualization/>; Accessed on Feb. 25, 2014; 5 pages.

DECT "Part 6: Identities and addressing" (1998-02) European Standard (Telecommunications series); 41 pages.

Domain Discover.US "Put Yourself on the Web"; Available at: <https://www.tierra.net/domains>; 3 pages.

Dropbox Review and Rating, Available at: <http://www.pcmag.com/article2/0,2817,2343852,00.asp>, Accessed on Feb. 25, 2014, 12 pages.

Fielding et al. (1999) "Hypertext Transfer Protocol—HTTP/1.1" Network Working Group; 114 pages.

Google website; Available at: <https://www.google.com/>; Accessed on Oct. 2, 2014; 1 page.

Google "Google Apps for Business" 2 pages, Available at: <http://www.google.com/enterprise/apps/business/>, Accessed on Feb. 28, 2014.

Google "Google Play" 3 pages, Available at: <https://play.google.com/store?hl=en>, Accessed on Feb. 28, 2014.

HD Wi-Fi video monitoring cameras for iPhone, Android or computer; Dropcam, Inc., Available at: <http://web.archive.org/web/20121213184724/https://www.dropcam.com/>; Accessed on Feb. 28, 2014, 3 pages.

Information Sciences Institute (1981) "Internet Protocol"; Available at: <http://www.ietf.org/rfc/rfc791.txt>; Accessed on Oct. 2, 2014; 48 pages.

International Telecommunication Union; E.164: The international public telecommunication numbering plan; Available at: <http://www.itu.int/rec/T-REC-E.164/en>; Accessed on Oct. 2, 2014; 1 page.

International Telecommunication Union; G.711: Pulse code modulation (PCM) of voice frequencies; Available at: <http://www.itu.int/rec/T-REC-G.711>; Accessed on Oct. 2, 2014; 1 page.

International Telecommunication Union; G.722: 7kHz audio-coding within 64 kbit/s; Available at: <http://www.itu.int/rec/T-REC-G.722>; Accessed on Oct. 2, 2014; 1 page.

IP Version 6 Working Group (ipv6); Available at: <http://datacenter.ietf.org/wg/ipv6 charter/>; Accessed on Oct. 2, 2014; 3 pages.

ITU-T (2007) "H.264 Series H: Audiovisual and Multimedia Systems"; 564 pages.

Johnny Chung Lee Projects—Wii www.johnnylee.net/projects/wii/ Accessed on Sep. 5, 2013, 3 pages.

Lifesize; Video Conference Systems and Accessories; Available at: <http://www.lifesize.com/en/products/video-conferencing-systems-and-accessories>; Accessed on Oct. 2, 2014; 11 pages.

Linux Foundation, "Why the Xen Project?", Available at: <http://www.xenproject.org/users/why-the-xen-project.html>, Accessed on Feb. 25, 2014, 5 pages.

Logitech Business Webcams; Available at: <http://www.logitech.com/en-us/for-business/products/webcams>; Accessed on Oct. 2, 2014; 4 pages.

Ludwig, XEP-0166: Jingle; Available at: <http://xmpp.org/extensions/xep-0166.html>; Accessed on Oct. 2, 2014; 49 pages.

Mahy et al. (2010) Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN); Available at: <http://tools.ietf.org/html/rfc5766>; Accessed on Oct. 2, 2014; 134 pages.

Microsoft, Xbox Games and Entertainment on All Your Devices; Available at: http://www.xbox.com/en-US/#fbid=__oRvaiAGfk1; Accessed on Oct. 2, 2014; 2 pages.

Nest, Learning Thermostat™ User Guide, 8 pages.

Netflix "Watch TV Shows Online, Watch Movies Online"; Available at: <https://www.netflix.com/?locale=en-US>; Accessed on Feb. 28, 2014; 1 page.

Nielson People Meters; Available at: <http://www.nielsen.com/content/corporate/us/en/solutions/measurement/television.html> Accessed on Oct. 2, 2014; 4 pages.

Notification Concerning Availability of Publication of the International Application; PCT Patent Application No. PCT/US2013/075184; mailed Jun. 19, 2014; 1 page.

Notification Concerning Availability of Publication of the International Application; PCT Patent Application No. PCT/US2013/075185; mailed Jun. 19, 2014; 1 page.

Notification Concerning Availability of Publication of the International Application; PCT Patent Application No. PCT/US2013/075186; mailed Jun. 19, 2014; 1 page.

Notification Concerning Availability of Publication of the International Application; PCT Patent Application No. PCT/US2014/014321; mailed Aug. 7, 2014; 1 page.

Notification of Transmittal of the International Search Report and the Written Opinion of the International Searching Authority, or the Declaration for PCT International Application No. PCT/US13/075184; mailed May 13, 2014; 15 pages.

Notification of Transmittal of the International Search Report and the Written Opinion of the International Searching Authority, or the Declaration for PCT International Application No. PCT/US13/075185; mailed Apr. 7, 2014; 12 pages.

Notification of Transmittal of the International Search Report and the Written Opinion of the International Searching Authority, or the Declaration for PCT International Application No. PCT/US13/75186; mailed May 1, 2014; 11 pages.

Notification of Transmittal of the International Search Report and the Written Opinion of the International Searching Authority, or the Declaration for PCT International Application No. PCT/US14/14321; mailed May 9, 2014; 18 pages.

Nyren, The Akamai Network: A Platform for High-Performance Internet Applications, Akamai Technologies, Cambridge, US, 18 pages.

Oracle VM VirtualBox, 2 pages, Available at: <https://www.virtualbox.org/>, Accessed on Feb. 25, 2014.

Panasonic (2011) Operating Instructions: KX-TG9471 and KX-TG9472; 64 pages.

(56)

References Cited**OTHER PUBLICATIONS**

Pantos et al. (2013) "HTTP Live Streaming"; Available at: <http://tools.ietf.org/html/draft-pantos-http-live-streaming-11>; Accessed on Oct. 2, 2014; 74 pages.

Polycom Data Sheet; Polycom® VoiceStation® 300 "Crystal-clear conferencing for smaller rooms and desktops"; 2013 Polycom, Inc.; 2 pages.

Polycom; Polycom HDX Series Product Brochure; Available at: <http://www.polycom.com/content/dam/polycom/common/documents/brochures/hdx-family-br-enus.pdf>; Accessed on Oct. 2, 2014; 4 pages.

Polycom User Guide; VoiceStation™ 300; Polycom, Inc. <http://www.polycom.com>; 17 pages.

Postel (1982) "Simple Mail Transfer Protocol" Info Sciences Institute, USC; 71 pages.

QEMU, Open Source Processor Emulator, 2 pages, Available at: http://wiki.qemu.org/Main_Page, Accessed on Mar. 4, 2014.

ROKU, User Guide (2008-2009), 51 pages, Roku, Inc.

Rosenberg (2010) "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols"; Available at: <http://tools.ietf.org/html/rfc5245>; Accessed on Oct. 12, 2014; 234 pages.

Rosenberg et al. "Session Traversal Utilities for NAT (STUN)"; Available at: <http://tools.ietf.org/html/rfc5389>; Accessed on Oct. 12, 2014; 102 pages.

Rosenberg, et al. (2002) "SIP: Session Initiation Protocol" <http://www.ietf.org/rfc/rfc3261.txt>; Accessed on Jun. 27, 2014; 265 pages.

Rosenberg "SIMPLE Made Simple: An Overview of the IETF Specifications for Instant Messaging and Presence Using the Session Initiation Protocol (SIP)" (Apr. 2013) Available at: <https://tools.ietf.org/html/rfc6914>, Accessed on Feb. 28, 2014.

Saint-Andre, "Extensible Messaging and Presence Protocol (XMPP): Core, Jabber Software Foundation" (Oct. 2004) 73 pages, Available at: <http://xmpp.org/rfcs/rfc3920.html>, Accessed on Feb. 28, 2014.

Skype video calling service; Available at: www.skype.com/en/; Accessed on Oct. 2, 2014; 4 pages.

Softlayer Services®, 2 pages, Available at: <http://www.softlayer.com/services/storagelayer>, Accessed on Mar. 4, 2014.

SPEEX: A Free Codec for Free Speech; Available at: <http://www.speex.org>; Accessed on Oct. 12, 2014; 2 pages.

U.S. Appl. No. 12/561,165; Notice of Allowance dated Feb. 2, 2012; 12 pages.

U.S. Appl. No. 13/857,736; Notice of Publication dated Oct. 10, 2013; 1 page.

U.S. Appl. No. 13/857,736; Ex Parte Quayle Office Action dated Sep. 16, 2014; 8 pages.

U.S. Appl. No. 14/106,263; NonFinal Office Action dated Mar. 6, 2014; 20 pages.

U.S. Appl. No. 14/106,263; Final Office Action dated Jun. 13, 2014; 21 pages.

U.S. Appl. No. 14/106,263; Notice of Publication dated Jun. 19, 2014; 1 page.

U.S. Appl. No. 14/106,279; NonFinal Office Action dated Feb. 28, 2014; 16 pages.

U.S. Appl. No. 14/106,279; Notice of Publication dated Jun. 19, 2014; 1 page.

U.S. Appl. No. 14/106,279; Final Office Action dated Jul. 22, 2014; 17 pages.

U.S. Appl. No. 14/106,360; NonFinal Office Action dated Mar. 20, 2014; 22 pages.

U.S. Appl. No. 14/106,360; Notice of Publication dated Jun. 19, 2014; 1 page.

U.S. Appl. No. 14/341,009, filed Jul. 25, 2014; 89 pages.

U.S. Appl. No. 14/464,435, filed Aug. 20, 2014; 111 pages.

U.S. Appl. No. 14/472,133, filed Aug. 28, 2014; 123 pages.

U.S. Appl. No. 14/479,169, filed Sep. 5, 2014; 99 pages.

Varia et al., Overview of Amazon Web Services (Jan. 2014), 22 pages, Amazon Web Services.

Variable Frame Rate MP4; https://kb.speeddemosarchive.com/Variable_Frame_Rate_MP4; Accessed on Jun. 27, 2014; 3 pages.

Vidyo, "The Vidyo Experience"; Available at: <http://www.vidyo.com/products/use/>; Accessed on Oct. 2, 2014; 5 pages.

WebRTC; Available at: <http://www.webrtc.org>; Accessed on Oct. 2, 2014; 4 pages.

WebSocket.org, Are you plugged in?; "What is WebSocket?"; Available at: <http://www.websocket.org>; Accessed on Oct. 2, 2014; Kaazing Corporation; 1 page.

Wikipedia, the free encyclopedia, Apache HTTP Server, 5 pages, Available at: http://en.wikipedia.org/wiki/Apache_HTTP_Server, Accessed on Feb. 26, 2014.

Wikipedia, the free encyclopedia; "Audio to Video Synchronization" Available at: http://en.wikipedia.org/wiki/Audio_to_video_synchronization; Accessed on Jun. 27, 2014; 6 pages.

Wikipedia, the free encyclopedia; "Cloud computing" Available at: en.wikipedia.org/wiki/Cloud_computing; Retrieved Mar. 3, 2014; 34 pages.

Wikipedia, the free encyclopedia; "Cloud storage" Available at: en.wikipedia.org/wiki/Cloud-storage; Retrieved Mar. 3, 2014; 5 pages.

Wikipedia, the free encyclopedia; "cPanel" Available at: <http://en.wikipedia.org/wiki/Cpanel>; Accessed on Feb. 26, 2014; 4 pages.

Wikipedia, the free encyclopedia; "Distributed computing" Available at: http://en.wikipedia.org/wiki/Distributed_computing; Accessed on Feb. 26, 2014; 12 pages.

Wikipedia, the free encyclopedia; "Email" Available at: en.wikipedia.org/wiki/Email; Retrieved Mar. 3, 2014; 25 pages.

Wikipedia, the free encyclopedia; "Face Detection" Available at: http://en.wikipedia.org/wiki/Face_detection; Accessed on Feb. 28, 2014; 2 pages.

Wikipedia, the free encyclopedia; "Face Recognition System" Available at: http://en.wikipedia.org/wiki/Facial_recognition_system; Accessed on Feb. 28, 2014; 10 pages.

Wikipedia, the free encyclopedia; "Grid computing" Available at: http://en.wikipedia.org/wiki/Grid_computing; Accessed on Feb. 26, 2014; 12 pages.

Wikipedia, the free encyclopedia; "Hypertext Transfer Protocol" Available at: en.wikipedia.org/wiki/Http; Retrieved Mar. 3, 2014; 10 pages.

Wikipedia, the free encyclopedia; "MPEG-4 Part 14" container format; Available at: <http://en.wikipedia.org/wiki/MPEG-4>; Accessed on Jun. 27, 2014; 4 pages.

Wikipedia, the free encyclopedia, "PlayStation 4" Available at: http://en.wikipedia.org/wiki/PlayStation_4, Accessed on Feb. 25, 2014, 21 pages.

Wikipedia, the free encyclopedia; "Session Initiation Protocol" Available at: http://en.wikipedia.org/wiki/Session_Initiation_Protocol; Accessed Jun. 27, 2014; 6 pages.

Wikipedia, the free encyclopedia "SIMPLE" en.wikipedia.org/wiki/SIMPLE, retrieved Mar. 3, 2014, 3 pages.

Wikipedia, the free encyclopedia; "Speech Recognition" Available at: http://en.wikipedia.org/wiki/Speech_recognition; Accessed on Feb. 28, 2014; 14 pages.

Wikipedia, the free encyclopedia; "Time-lapse photography" Available at en.wikipedia.org/wiki/Time-lapse_photography; Retrieved Mar. 3, 2014; 11 pages.

Wikipedia, the free encyclopedia; "Transmission Control Protocol" Available at: en.wikipedia.org/wiki/Transmission_Control_Protocol; Retrieved Mar. 3, 2014; 19 pages.

Wikipedia, the free encyclopedia; "VP8" Available at: <http://en.wikipedia.org/wiki/VP8>; Retrieved Oct. 12, 2014; 8 pages.

Wikipedia, the free encyclopedia; "Wii" Available at: <http://en.wikipedia.org/wiki/Wii>; Accessed on Feb. 25, 2014; 30 pages.

Wikipedia, the free encyclopedia; "Wolfram Alpha" Available at: http://en.wikipedia.org/wiki/Wolfram_Alpha; Accessed on Feb. 25, 2014; 6 pages.

Wikipedia, the free encyclopedia; "Xbox One" Available at: http://en.wikipedia.org/wiki/Xbox_one; Accessed on Feb. 25, 2014; 16 pages.

Wikipedia, the free encyclopedia; "XMPP" Available at: en.wikipedia.org/wiki/XMPP; Retrieved Mar. 3, 2014; 10 pages.

(56)

References Cited**OTHER PUBLICATIONS**

XMPP Standards Foundation; Available at: <http://xmpp.org/xmpp-protocols/>; Accessed on Oct. 2, 2014; 1 page.

Young (1998) "FundamentalsImageProcessing," 113 pages.

Zoom Video Communications, Inc.; Zoom Cloud Video Conferencing; Available at: <http://www.zoom.us>; Accessed on Oct. 2, 2014; 2 pages.

Google "How Set Up Google Chromecast?" Available at googlechromecast.com/how-set-up-google-chromecast/, retrieved on Apr. 29, 2014, 25 pages.

Google "What is Google Chromecast?" Available at googlechromecast.com/what-is-google-chromecast/ retrieved on Apr. 29, 2014, 6 pages.

Notification Concerning Transmittal of International Preliminary Report on Patentability by the International Bureau of WIPO for PCT International Application No. PCT/US13/75184; mailed Jun. 25, 2015; 11 pages.

Notification Concerning Transmittal of International Preliminary Report on Patentability by the International Bureau of WIPO for PCT International Application No. PCT/US13/75185; mailed Jun. 25, 2015; 9 pages.

Notification Concerning Transmittal of International Preliminary Report on Patentability by the International Bureau of WIPO for PCT International Application No. PCT/US13/75186; mailed Jun. 25, 2015; 8 pages.

Notification of Transmittal of the International Search Report and the Written Opinion of the International Searching Authority, or the Declaration for PCT International Application No. PCT/US14/48158; mailed Nov. 10, 2014; 12 pages.

Notification of Transmittal of the International Search Report and the Written Opinion of the International Searching Authority, or the Declaration for PCT International Application No. PCT/US14/53254; mailed Dec. 15, 2014; 11 pages.

Notification of Transmittal of the International Search Report and the Written Opinion of the International Searching Authority, or the Declaration for PCT International Application No. PCT/US14/54409; mailed Dec. 16, 2014; 16 pages.

U.S. Appl. No. 14/106,263; NonFinal Office Action dated Mar. 24, 2015; 48 pages.

U.S. Appl. No. 14/106,279; NonFinal Office Action dated Mar. 20, 2015; 30 pages.

U.S. Appl. No. 14/106,360; Notice of Allowance dated Oct. 29, 2014; 22 pages.

U.S. Appl. No. 14/341,009; NonFinal Office Action dated Apr. 22, 2015; 39 pages.

U.S. Appl. No. 14/464,435; NonFinal Office Action dated Feb. 12, 2015; 33 pages.

U.S. Appl. No. 14/472,133; NonFinal Office Action dated Feb. 11, 2015; 34 pages.

Wikipedia, the free encyclopedia; "Bluetooth" Available at: en.wikipedia.org/wiki/Bluetooth; retrieved on Apr. 29, 2014; 25 pages.

Wikipedia, the free encyclopedia; "Wi-Fi Direct" Available at: en.wikipedia.org/wiki/Wi-Fi_Direct; Retrieved on Apr. 29, 2014; 5 pages.

U.S. Appl. No. 14/106,263; Notice of Allowance dated Sep. 25, 2015; 24 pages.

U.S. Appl. No. 14/341,009; Final Office Action dated Oct. 8, 2015; 35 pages.

U.S. Appl. No. 14/464,435; Final Office Action dated Sep. 21, 2015; 26 pages.

U.S. Appl. No. 14/472,133; Final Office Action dated Sep. 22, 2015; 26 pages.

U.S. Appl. No. 14/479,169; NonFinal Office Action dated Sep. 18, 2015; 76 pages.

U.S. Appl. No. 14/106,279; Final Office Action dated Aug. 3, 2015; 23 pages.

U.S. Appl. No. 14/539,106; NonFinal Office Action dated Sep. 15, 2015; 45 pages.

Notification Concerning Transmittal of International Preliminary Report on Patentability by the International Bureau of WIPO for PCT International Application No. PCT/US14/14321; mailed Aug. 13, 2015; 11 pages.

U.S. Appl. No. 14/106,279; Notice of Allowance dated Dec. 3, 2015; 16 pages.

Notification Concerning Transmittal of International Preliminary Report on Patentability by The International Bureau of WIPO for PCT International Application No. PCT/US14/48158; dated Jan. 26, 2015; 9 pages.

* cited by examiner

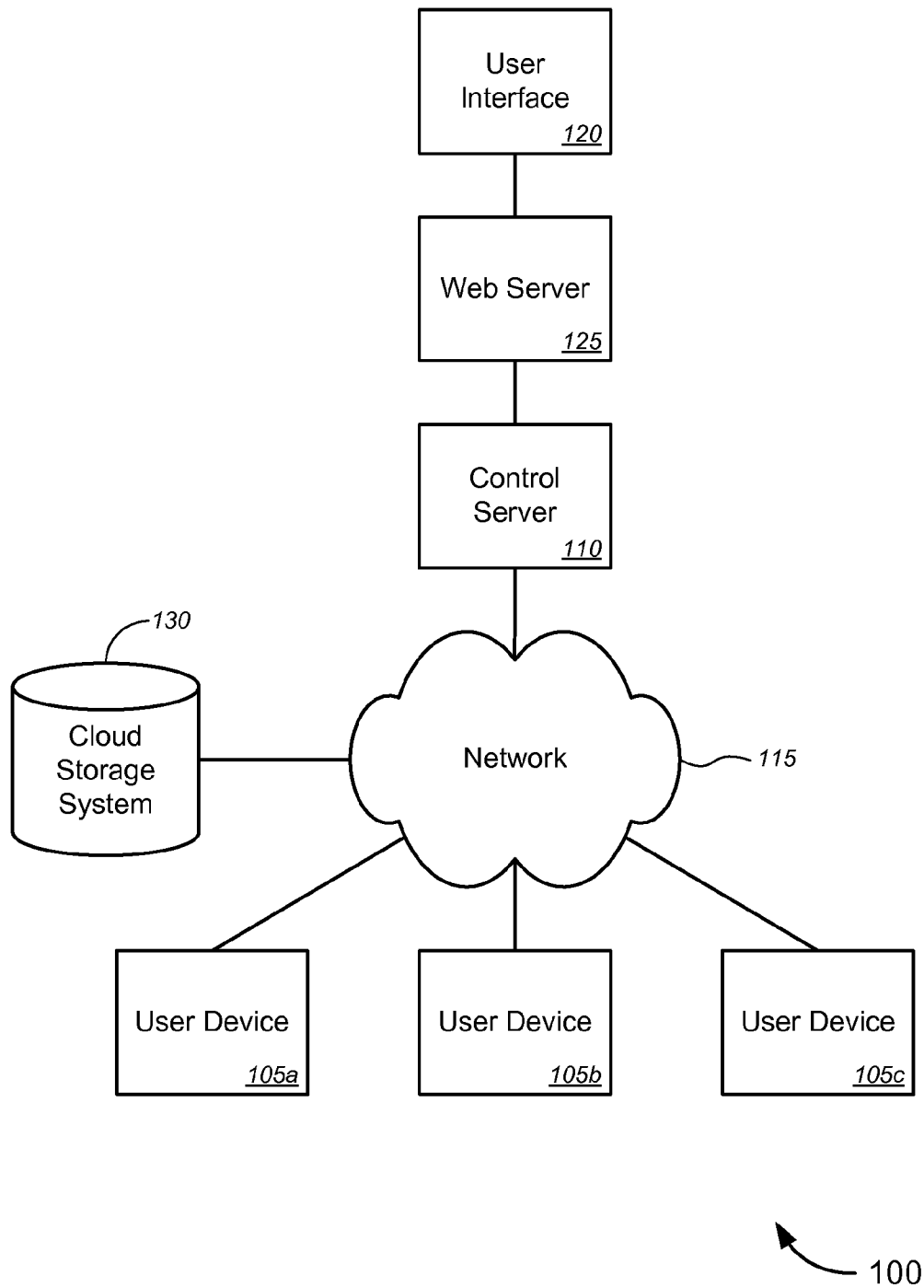


Fig. 1

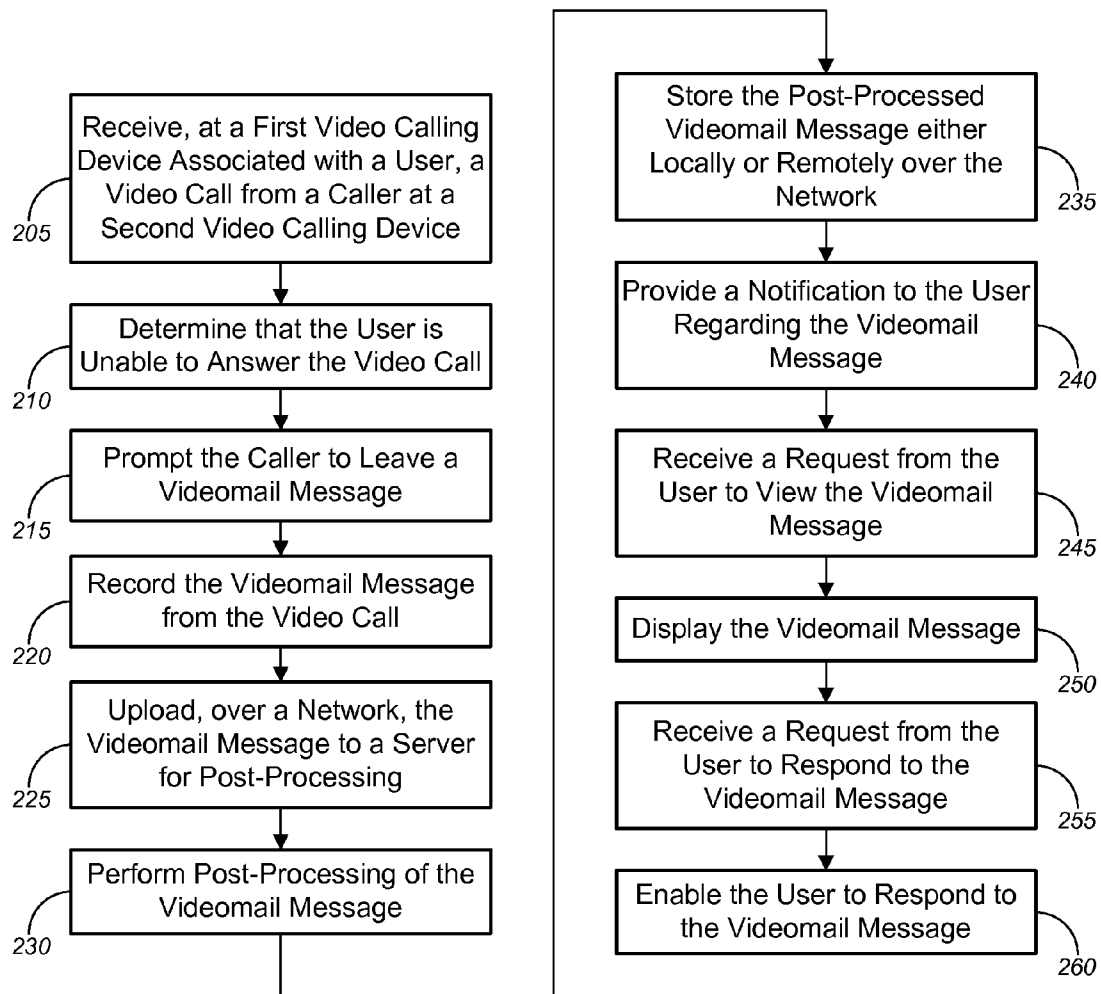


Fig. 2

200

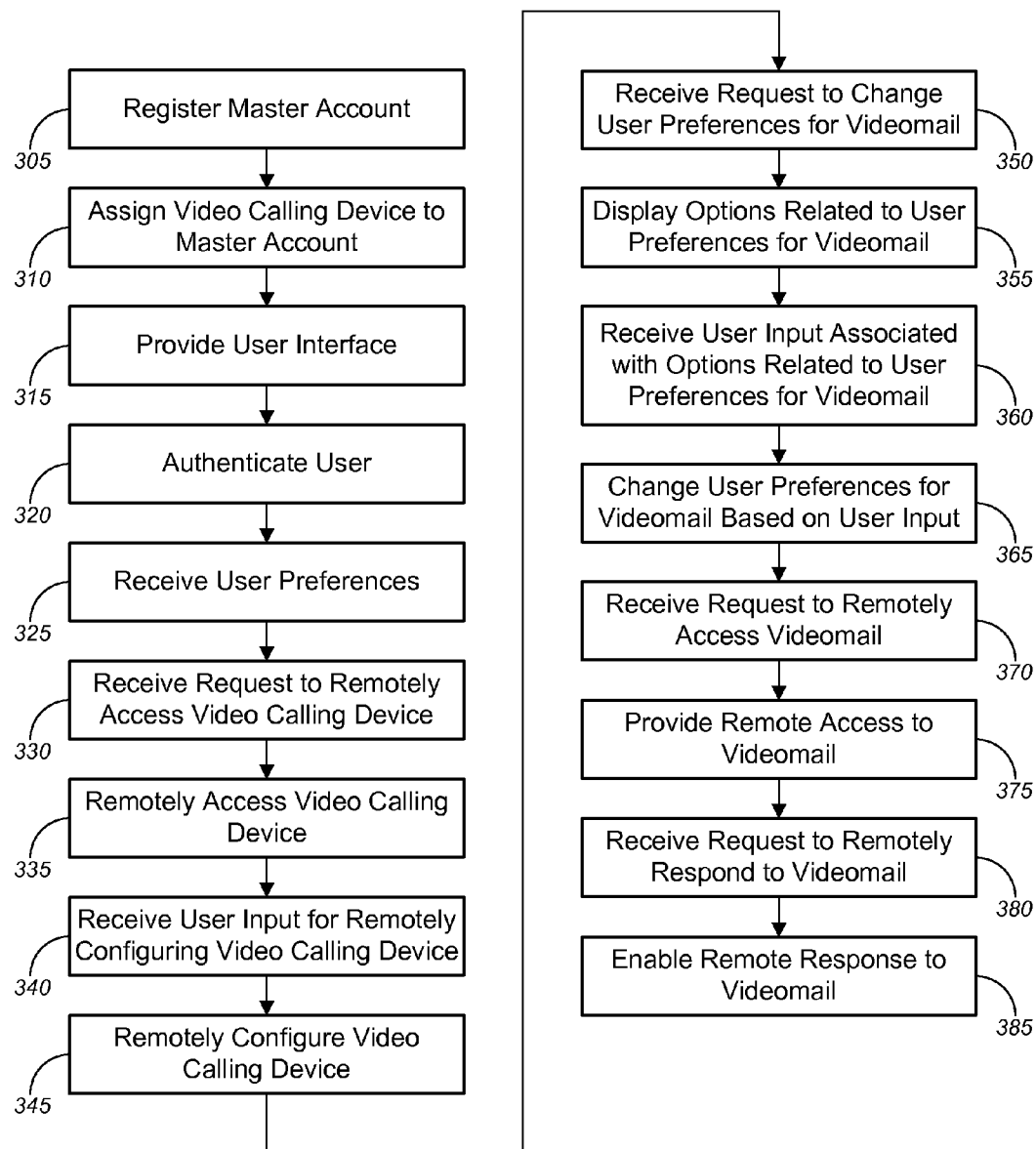


Fig. 3

300

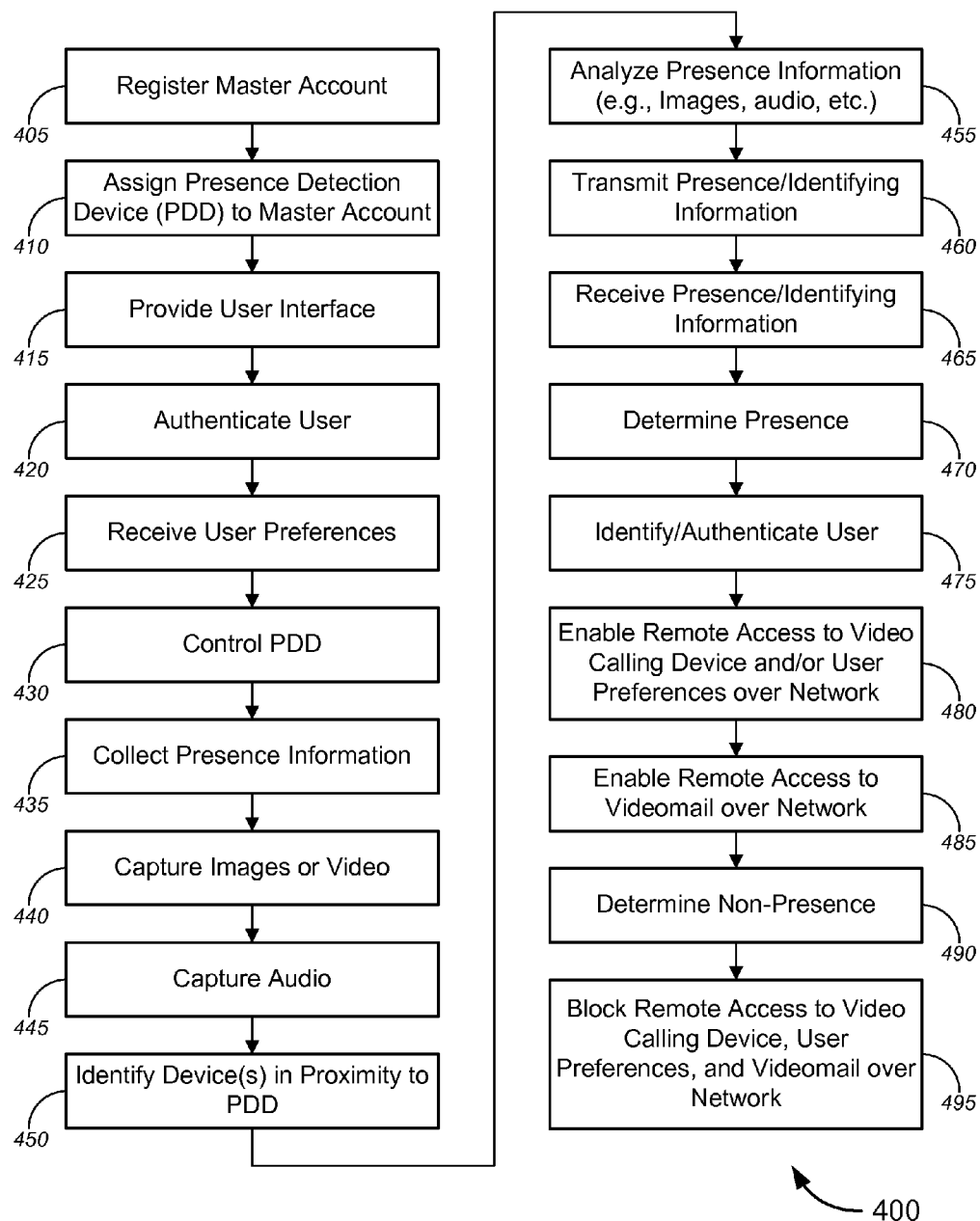
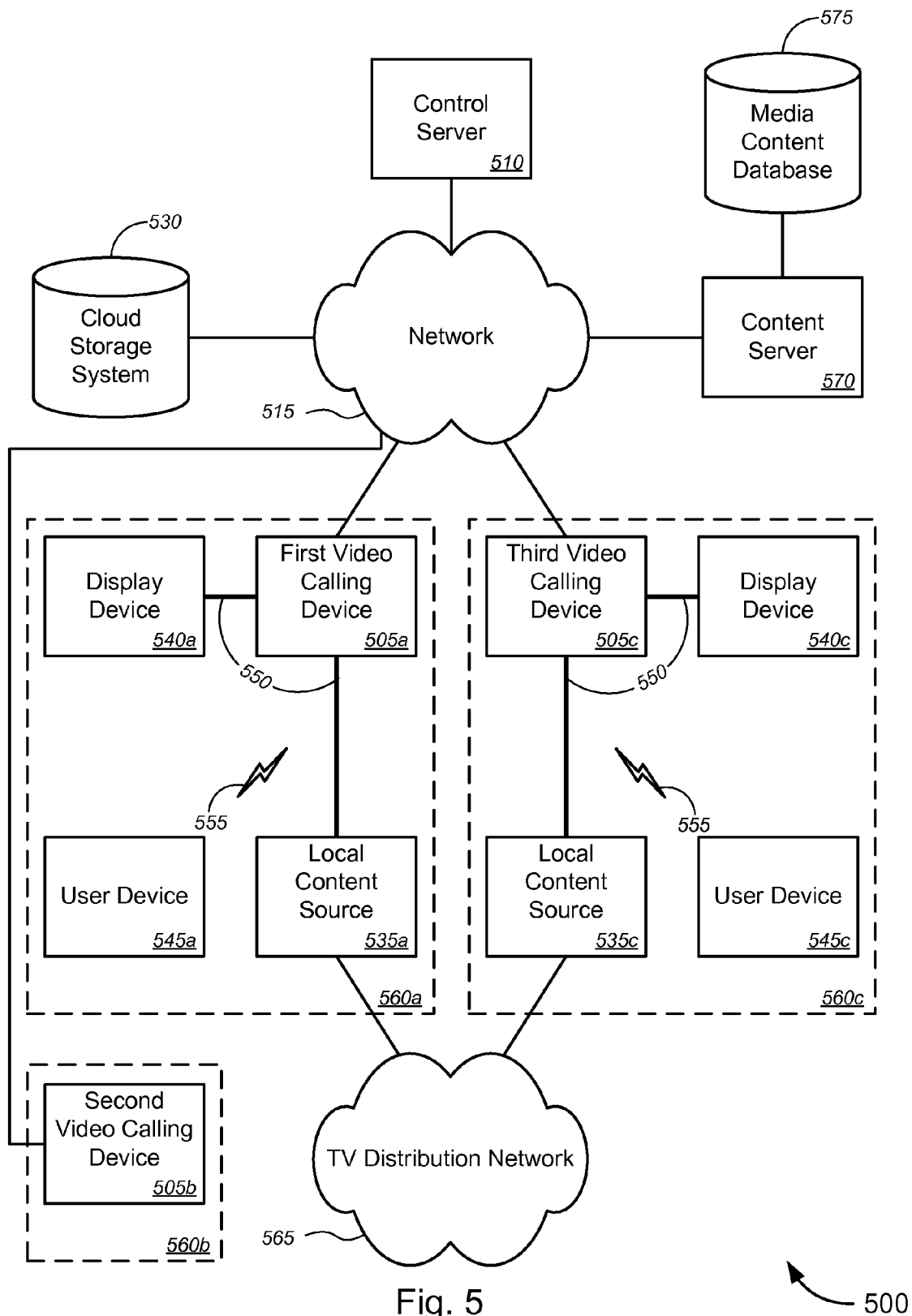


Fig. 4



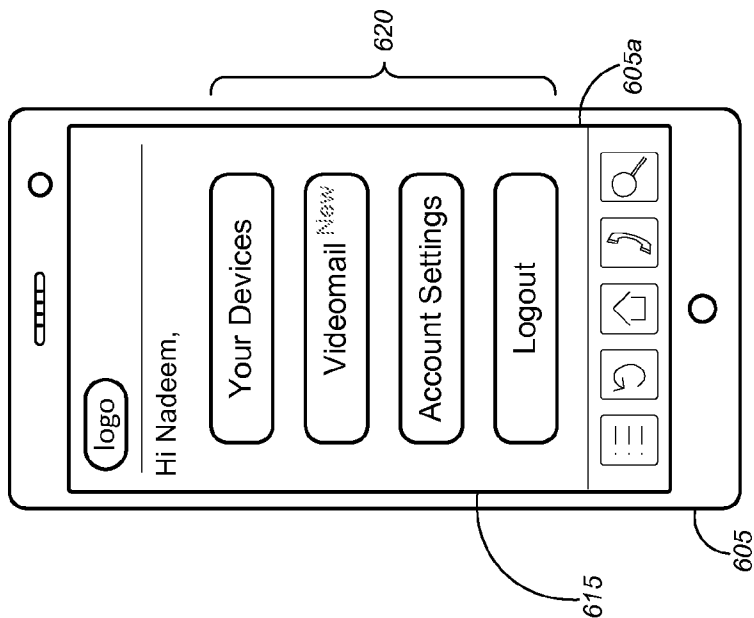


FIG. 6A

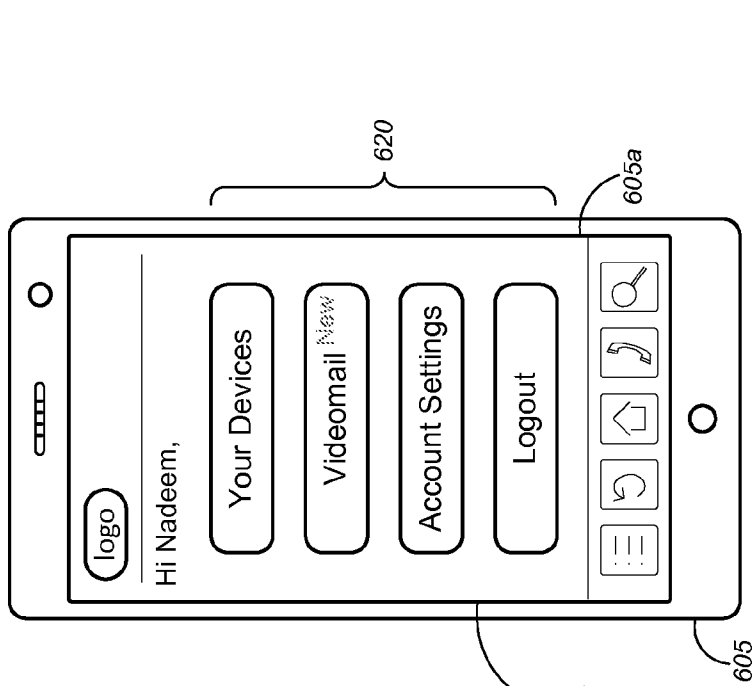


FIG. 6B

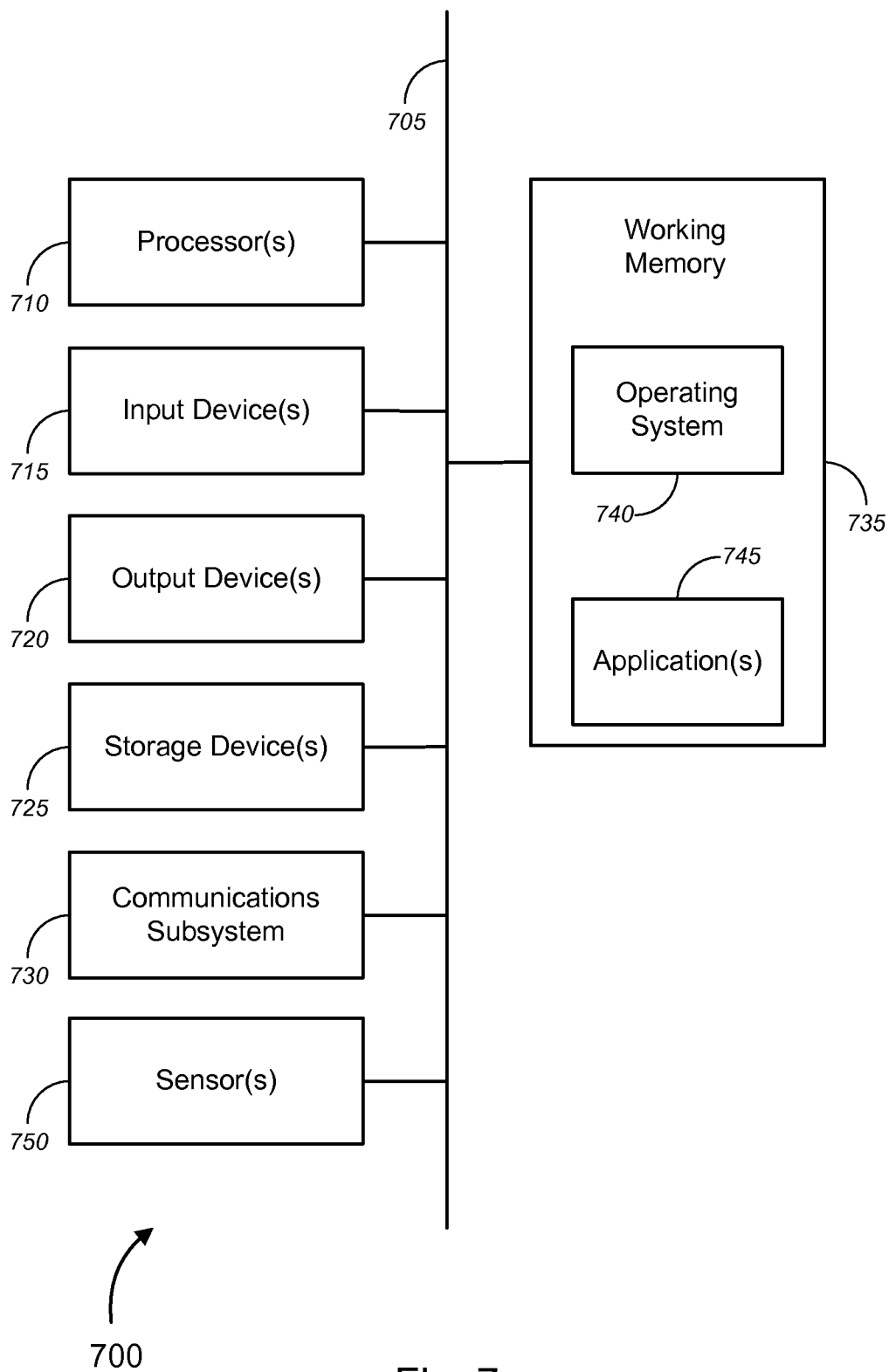


Fig. 7

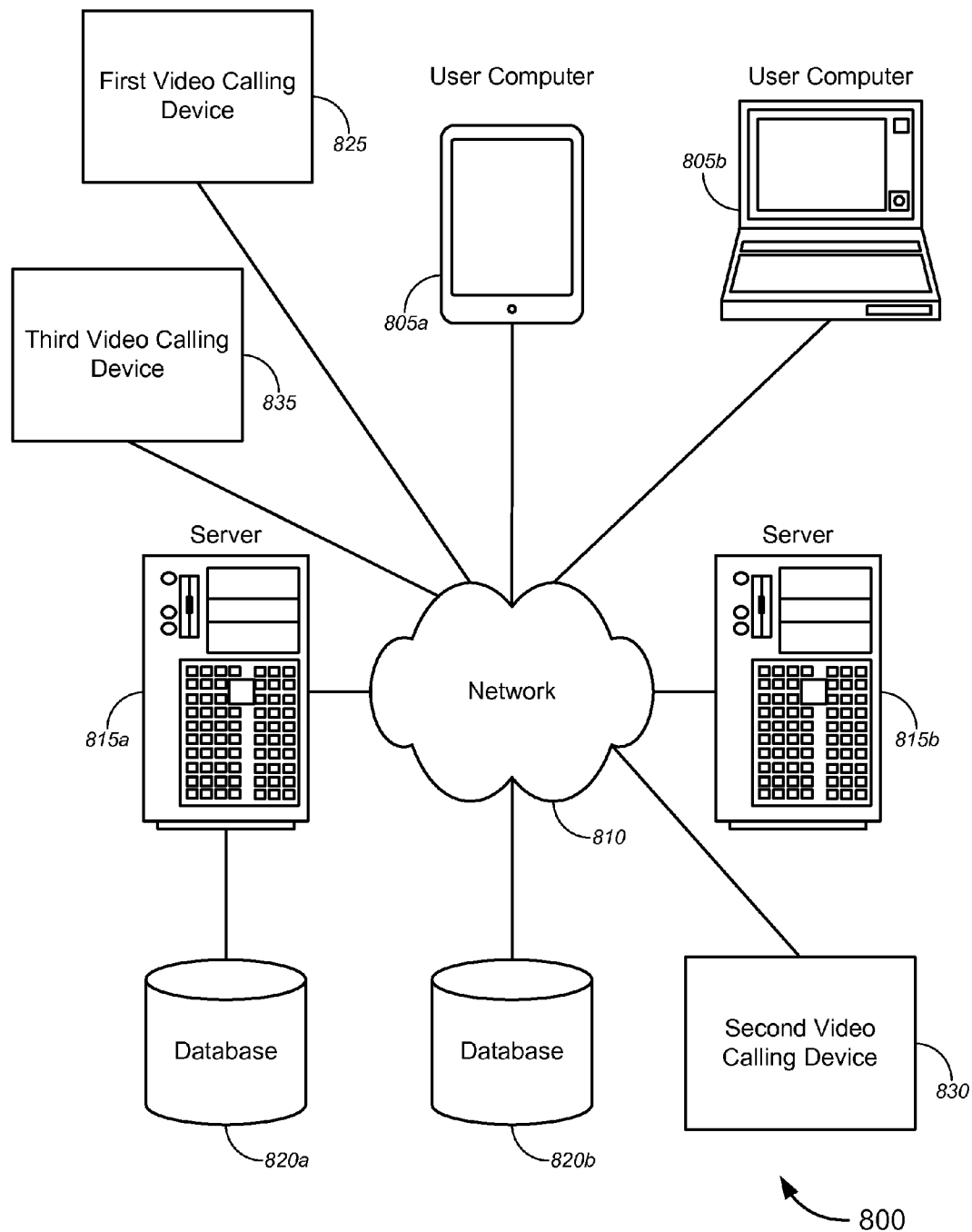


Fig. 8

1

VIDEO MAIL CAPTURE, PROCESSING AND DISTRIBUTION

CROSS-REFERENCES TO RELATED APPLICATIONS

This application claims the benefit, under 35 U.S.C. §119 (e), of the following applications: provisional U.S. Patent Application No. 61/877,928, filed Sep. 13, 2013 by Ahmed et al. and titled "Mobile Presence Detection" provisional U.S. Patent Application No. 61/874,903, filed Sep. 6, 2013 by Shoemake et al. and titled "Virtual Window" provisional U.S. Patent Application No. 61/872,603, filed Aug. 30, 2013 by Shoemake et al. and titled "Physical Presence and Advertising"; provisional U.S. Patent Application No. 61/858,518, filed Jul. 25, 2013 by Shoemake et al. and titled "Video Calling and Conferencing Advertising"; and provisional U.S. Patent Application No. 61/759,621, filed Feb. 1, 2013 by Shoemake et al. and titled "Video Mail Capture, Processing and Distribution". This application is a continuation-in-part of U.S. patent application Ser. No. 14/106,263, filed on Dec. 13, 2013 by Shoemake et al. and titled "Video Capture, Processing and Distribution System", which claims the benefit of provisional U.S. Patent Application No. 61/737,506, filed Dec. 14, 2012 by Shoemake et al. and titled "Video Capture, Processing and Distribution System" This application is also a continuation in part of U.S. patent application Ser. No. 14/106,279, filed on Dec. 13, 2013 by Ahmed et al. and titled "Mobile Presence Detection" and U.S. patent application Ser. No. 14/106,360, filed on Dec. 13, 2013 by Ahmed et al. and titled "Distributed Infrastructure".

The respective disclosures of these applications/patents (which this document refers to collectively as the "Related Applications") are incorporated herein by reference in their entirety for all purposes.

COPYRIGHT STATEMENT

A portion of the disclosure of this patent document contains material that is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure as it appears in the Patent and Trademark Office patent file or records, but otherwise reserves all copyright rights whatsoever.

FIELD

The present disclosure relates, in general, to video calling, and, more particularly, to tools and techniques for enabling or implementing video mail capture, processing, and distribution.

BACKGROUND

The proliferation of capable user devices, pervasive communication, and increased bandwidth has provided opportunity for many enhanced services for users. One example is video calling. Once the domain of high-end, dedicated systems from vendors such as POLYCOM®, video calling has become available to the average consumer at a reasonable cost. For example, the Biscotti™ device, available from Biscotti, Inc., provides an inexpensive tool to allow video calling using a high-definition television and an Internet connection. More generally, a class of devices, which have been described as "video calling devices" but are referred to herein as video communication devices ("VCDs") can be simultaneously

2

connected to a display (such as a television, to name one example) and a source of content (such as a set-top box ("STB"), to name an example) in a pass-through configuration and can have a network connection and/or sensors such as a camera, a microphone, infrared sensors, and/or other suitable sensors. Such devices present a powerful platform for various applications. Examples include, without limitation, video calling, instant messaging, presence detection, status updates, media streaming over the Internet, web content viewing, gaming, and DVR capability. Another example of such value added services is the introduction of online gaming. Rather than playing a game by him- or herself, a user now can play most games in a multiplayer mode, using communication over the Internet or another network.

Enabling such services is a new class of user device, which generally features relatively high-end processing capability (which would have been unthinkable outside supercomputing labs just a few years ago), substantial random access memory, and relatively vast non-transient storage capabilities, including hard drives, solid state drives, and the like. Such user devices can include, without limitation, the VCDs mentioned above, the presence detection devices ("PDDs") described in the '279 application, various video game consoles, and the like. Such devices generally have a reliable, and relatively high-speed, connection to the Internet (to enable the value added services) and significant amounts of downtime, in which the processing and other capabilities of the devices are unused.

Additionally, some existing products offer video mail. However, implementation of such existing video mail services depend on both parties (i.e., caller and callee) to have the same product because such existing products are based on the calling device recording the video mail and thus must be able to intercommunicate with (or otherwise be compatible with) the called device in order to record and leave a video mail. This is a major limitation as the caller (the person leaving the video mail) must also have the same product as the callee, which limits the utility of the video mail feature.

Hence, there is a need for solutions that allow for more flexible video mail implementations, and/or for more flexible configuration options thereof, as well as for more flexible remote access to video mail, and some such solutions can employ the powerful user devices already resident in many users' homes.

BRIEF SUMMARY

A set of embodiments provides tools and techniques for enabling or implementing video mail capture, processing, and distribution.

In some embodiments, the video mail or video mail data (hereinafter also referred to as "videomail" and "videomail data," respectively) may be post-processed on a computer in the network, which can include a control server(s), a central server(s), another image capture device(s), and/or the like. In some cases, distributed hosting, including cloud-based computing, cloud-based application hosting, cloud-based data storage, and/or content delivery network service, or the like, as described in detail in the '360 application (already incorporated herein) may be utilized to perform post-processing of video mail or video mail data, to store raw as well as processed video mail data, to share video mail data captured by the Internet-connected cameras (including raw and processed video and/or images), to host a website for allowing a user to control such functionalities, to access the video mail, and/or the like.

In some instances, presence detection techniques and presence detection devices ("PDDs") described in detail in the '279 application may be used to allow for automatic identification and authentication to enable the user to establish or modify preferences or settings for video mail, to initiate post-processing of captured video mail data, to instruct storing of raw as well as processed video mail data, to share video mail data captured by the Internet-connected cameras (including raw and processed video mail data), to control such functionalities, and/or the like, regardless of where the user is, so long as the user is in front of a suitable device capable of identification and authentication of the user to provide the user access to a master account for controlling these functionalities. In other words, a profile for accessing control of the above-mentioned functionalities (as well as the (raw/processed) captured video mail data) can follow the user.

The tools provided by various embodiments include, without limitation, methods, systems, and/or software products. Merely by way of example, a method might comprise one or more procedures, any or all of which are executed by a video calling device, a PDD, and/or a computer system. Correspondingly, an embodiment might provide a video calling device, a PDD, and/or a computer system configured with instructions to perform one or more procedures in accordance with methods provided by various other embodiments. Similarly, a computer program might comprise a set of instructions that are executable by a video calling device, a PDD, and/or a computer system (and/or a processor therein) to perform such operations. In many cases, such software programs are encoded on physical, tangible, and/or non-transitory computer readable media (such as, to name but a few examples, optical media, magnetic media, and/or the like).

In an aspect, a method might comprise receiving, at a first video calling device associated with a user and over a network, a video call from a caller at a second video calling device. The method might also comprise determining, with one or both of the first video calling device or the second video calling device, that the user is unable to answer the video call. The method might further comprise recording, with the first video calling device that receives the call, a videomail message from the video call, based at least in part on a determination that the user is unable to answer the video call. In some embodiments, the method might further comprise prompting, with the first video calling device associated with the user, the caller to leave the videomail message.

According to some embodiments, the first video calling device and the second video calling device are at least one of made by different manufacturers or of different models of calling device.

In some embodiments, the method might comprise uploading, over the network, at least a portion of the videomail message to a server for post-processing. In some cases, uploading, over the network, at least a portion of the videomail message to a server for post-processing might comprise uploading at least a portion of each of one or more components of the videomail message. The one or more components of the videomail message might comprise an audio component, a video component, and a timecode component. In some instances, post-processing might comprise scaling video of the videomail message to a specified resolution. Alternatively, or additionally, post-processing might comprise mixing audio and video of the videomail message by reference to a timecode. In other instances, post-processing might comprise adding a visible watermark to the videomail message. In some cases, post-processing might comprise formatting the videomail message as a video viewable by a web browser. Post-processing might also comprise formatting the video-

mail message for downloading by the user, or formatting the videomail message for viewing on a user device.

According to some aspects, the method might further comprise providing a notification to the user regarding the videomail message. In some embodiments, the notification might comprise an e-mail message with a link to a formatted video comprising the videomail message. In some instances, the method might further comprise creating a uniform resource locator ("URL") addressing the formatted video. The link might include the URL addressing the formatted video. Alternatively, the notification might comprise an e-mail message, in which the videomail message is one of an attached videomail message or an embedded videomail message. In yet another alternative, the notification might comprise a text message (including, without limitation, a short message service ("SMS") message, a multimedia message service ("MMS"), and/or the like) with a link to a formatted video comprising the videomail message.

In some embodiments, the method might comprise recording a timecode file to a storage medium at one of the first video calling device, the second video calling device, or the server. The timecode file might indicate when each frame of video of the videomail message should be displayed and indicating when each frame of audio of the videomail message should be played. The method might further comprise synchronizing, at the one of the first video calling device, the second video calling device, or the server, audio and video from the videomail message, based at least in part on the recorded timecode file. In some cases, uploading the videomail message to the server might comprise uploading an audio file, a video file, and the timecode to the server.

According to some embodiments, each of at least one of the first video calling device or the second video calling device might comprise a first video input interface to receive first video input from a first local content source, a first audio input interface to receive first audio input from the first local content source, a first video output interface to provide first video output to a first video display device, a first audio output interface to provide first audio output to a first audio receiver, a first video capture device to capture at least one of first image data or first video data, a first audio capture device to capture first audio data, a first network interface, at least one first processor, and a first storage medium in communication with the at least one first processor.

The method, in some embodiments, might further comprise registering, with a first computer, a master account for the user, assigning, with the first computer, the first video calling device to the master account, authenticating the user, at the first computer, using a set of credentials associated with the master account, and accessing the first video calling device from the first computer, over the network, after authenticating the user. The method might also comprise providing a user interface, from the first computer, over the network, and receiving, by the first computer, user input associated with options presented by the user interface. The options might include one or more of options for establishing user preferences for videomail messages, options for modifying user preferences for videomail messages, options for deleting user preferences for videomail messages, options for notifying the user regarding videomail messages, or options for responding to videomail messages. The network, in some instances, is the Internet, and the user interface comprises a web page. In some embodiments, the method might further comprise receiving a request from the user to view the videomail message and displaying the videomail message with the user interface.

According to some embodiments, the first computer is one of the first video calling device or the second video calling

5

device. In some instances, receiving user input might comprise receiving user input from a third video calling device. The third video calling device might comprise a second video input interface to receive second video input from a second local content source, a second audio input interface to receive second audio input from the second local content source, a second video output interface to provide second video output to a second video display device, a second audio output interface to provide second audio output to a second audio receiver, a second video capture device to capture at least one of second image data or second video data, a second audio capture device to capture second audio data, a second network interface, at least one second processor, and a second storage medium in communication with the at least one second processor. The method might further comprise providing the user with access, over the network, to at least one of the first video calling device or the master account.

In some embodiments, the method might further comprise collecting presence information with the third video calling device, detecting presence of the user, with the third video calling device, based at least in part on the presence information, identifying the user, with a second computer, based at least in part on identifying information derived from at least a portion of the presence information, and in response to identifying the user, providing, over the third video calling device, options for the user to view any videomail messages left for the user. In some instances, identifying the user might comprise one or more of analyzing, with the second computer, at least one of captured second image data or captured second video data, using facial recognition software; comparing, with the second computer, at least a portion of the captured second audio data with a voiceprint; comparing, with the second computer, at least a portion of the captured second audio data with stored challenge/response information; determining, with the second computer, whether a username and a password inputted by the user matches a pre-stored username and a pre-stored password associated with the user; determining, with the second computer, whether a user device that is detected in proximity to the presence detection device is a device associated with the user; or detecting a presence of a user device that is associated with the user, based on at least one of detecting a Bluetooth connection of the user device, detecting that the user device is associated with a WiFi access point with which the presence detection device has associated, or communicating with the user device using near field communication ("NFC").

In another aspect, an apparatus might comprise one or more processors and a computer readable medium in communication with the one or more processors. The computer readable medium might have encoded thereon a set of instructions executable by the one or more processors to cause the apparatus to perform one or more operations. The set of instructions might comprise instructions for receiving a video call from a video calling device, instructions for determining that the user is unable to answer the video call, and instructions for recording a videomail message from the video call, based at least in part on a determination that the user is unable to answer the video call.

In yet another aspect, a video calling device might comprise one or more processors and a computer readable medium in communication with the one or more processors. The computer readable medium might have encoded thereon a set of instructions executable by the one or more processors to cause the video calling device to perform one or more operations. The set of instructions might comprise instructions for instructions for sending a video call to an apparatus, instructions for determining that a callee associated with the

6

apparatus is not available to answer the video call, instructions for recording a videomail message from the video call, based at least in part on a determination that the callee is unable to answer the video call, and instructions to send a notification to the callee with instructions to access the videomail message.

In still another aspect, a system might comprise a first video calling device associated with a user and a server computer. The first video calling device might comprise one or more first processors and a first computer readable medium in communication with the one or more first processors. The first computer readable medium might have encoded thereon a first set of instructions executable by the one or more first processors to cause the first video calling device to perform one or more operations. The first set of instructions might comprise instructions for receiving a video call from a caller at a second video calling device, instructions for determining that the user is unable to answer the video call, instructions for recording a videomail message from the video call, based at least in part on a determination that the user is unable to answer the video call, and instructions for uploading the videomail message.

The server computer might comprise one or more second processors and a second computer readable medium in communication with the one or more second processors. The second computer readable medium might have encoded thereon a second set of instructions executable by the one or more second processors to cause the server computer to perform one or more operations. The second set of instructions might comprise instructions to receive the uploaded videomail message.

According to some embodiments, the second set of instructions might further comprise instructions to post-process the videomail message. In some cases, the second set of instructions might further comprise instructions to provide a notification to a callee regarding the videomail message.

Various modifications and additions can be made to the embodiments discussed without departing from the scope of the invention. For example, while the embodiments described above refer to particular features, the scope of this invention also includes embodiments having different combination of features and embodiments that do not include all of the above described features.

BRIEF DESCRIPTION OF THE DRAWINGS

A further understanding of the nature and advantages of particular embodiments may be realized by reference to the remaining portions of the specification and the drawings, in which like reference numerals are used to refer to similar components. In some instances, a sub-label is associated with a reference numeral to denote one of multiple similar components. When reference is made to a reference numeral without specification to an existing sub-label, it is intended to refer to all such multiple similar components.

FIG. 1 is a block diagram illustrating a system for enabling or implementing video mail capture, processing, and distribution, in accordance with various embodiments.

FIG. 2 is a process flow diagram illustrating a method of enabling or implementing video mail capture, processing, and distribution, in accordance with various embodiments.

FIG. 3 is a process flow diagram illustrating a method of enabling remote access to user preferences for videomail and enabling remote access to videomail, in accordance with various embodiments.

FIG. 4 is a process flow diagram illustrating a method of enabling remote access to a master account, to user prefer-

ences for videomail, and to videomail based on the presence of a user, in accordance with various embodiments.

FIG. 5 is a block diagram illustrating another system for enabling or implementing video mail capture, processing, and distribution, in accordance with various embodiments.

FIG. 6A is an illustration of a user device used by users that presents an exemplary graphical user interface for notifying users regarding videomail messages, in accordance with various embodiments.

FIG. 6B is an illustration of a user device used by users that present an exemplary graphical user interface for presenting options related to a user's master account, the user's devices, videomail, and account settings, in accordance with various embodiments.

FIG. 7 is a generalized schematic diagram illustrating a computer system, in accordance with various embodiments.

FIG. 8 is a block diagram illustrating a networked system of computers, which can be used in accordance with various embodiments.

DETAILED DESCRIPTION OF CERTAIN EMBODIMENTS

While various aspects and features of certain embodiments have been summarized above, the following detailed description illustrates a few exemplary embodiments in further detail to enable one of skill in the art to practice such embodiments. The described examples are provided for illustrative purposes and are not intended to limit the scope of the invention.

In the following description, for the purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the described embodiments. It will be apparent to one skilled in the art, however, that other embodiments of the present invention may be practiced without some of these specific details. In other instances, certain structures and devices are shown in block diagram form. Several embodiments are described herein, and while various features are ascribed to different embodiments, it should be appreciated that the features described with respect to one embodiment may be incorporated with other embodiments as well. By the same token, however, no single feature or features of any described embodiment should be considered essential to every embodiment of the invention, as other embodiments of the invention may omit such features.

Unless otherwise indicated, all numbers used herein to express quantities, dimensions, and so forth used should be understood as being modified in all instances by the term "about." In this application, the use of the singular includes the plural unless specifically stated otherwise, and use of the terms "and" and "or" means "and/or" unless otherwise indicated. Moreover, the use of the term "including," as well as other forms, such as "includes" and "included," should be considered non-exclusive. Also, terms such as "element" or "component" encompass both elements and components comprising one unit and elements and components that comprise more than one unit, unless specifically stated otherwise.

Features Provided by Various Embodiments Presence Detection Functionalities

Presence Detection Devices ("PDDs") provided by various embodiments can contain or communicate with, inter alia, cameras, microphones, and/or other sensors (including, without limitation, infrared ("IR") sensors). These sensors, in conjunction with the internal processing capability of the device, can allow the device to detect when a person is in the room. Additionally, through means such as facial recognition and voice detection, or the like, the devices also can automatically recognize who is in the room. More specifically, such

devices can detect the presence of a particular individual. In some aspects, Image Capture Devices ("ICDs") might contain or communicate with, inter alia, video capture devices for capturing video mail and/or video mail data. In some cases, ICDs might also contain or communicate with, inter alia, microphones, and/or other sensors (including, without limitation, infrared ("IR") sensors). According to some embodiments, some ICDs might have similar functionality as PDDs.

In various embodiments, presence detection can be local and/or cloud based. In the case of local presence detection, the PDD itself might keep a list of all user profiles and will attempt to match an individual against its local list of all users. In cloud based detection, the functionality of user detection can be moved into servers in the cloud. A cloud based approach allows detection of a user's presence to be mobile among various devices (whether or not owned by, and/or associated with, the user). That same user can be detected on their device or on any other device that has the same capability and that is tied into the same cloud infrastructure.

The ability to automatically detect the presence of an individual on any device presents a powerful new paradigm for many applications including automation, customization, content delivery, gaming, video calling, and others. Advantageously, in some embodiments, a user's content, services, games, profiles, videomail, e-mail, and/or preferences, etc. can follow that user from device to device, including devices that are not owned by (or previously associated with) the individual, as described in detail in the '279 application (already incorporated herein). Alternatively, or in addition, presence detection functionality can also allow for mobile presence detection that enables remote access and control of ICDs over a network, following automatic identification and authentication of the user by any device (e.g., PDD, ICD, or other device) so long as such device has authentication functionality that is or can be tied to the access and control of the ICDs, regardless of whether or not such device is owned or associated with the user. In other words, the ability to remotely access and control one's ICDs over a network can follow the user wherever he or she goes, in a similar manner to the user's content and profiles following the user as described in the '279 application. Such remote control of ICDs, as well as post-processing of video and/or image data captured by the ICDs, is described in detail in the '263 application (which is already incorporated by reference herein).

Various sensors on a PDD (and/or a video calling device) can be used for user detection. Facial recognition can be used to identify a particular individual's facial characteristics, and/or voice detection can be used to uniquely identify a person. Additionally, PDDs and/or ICDs may also have local data storage. This local data storage can be used to store a database of user profiles. The user profiles can contain the various mechanisms that can be used to identify a person, including username and password, facial characteristics, voice characteristics, etc. When sensors detect the facial features or capture the voice of a particular individual, that captured presence information can be compared against the characteristics of the users on the local storage. If a match is found, then the individual has been successfully identified by the device. (As used herein, the term "presence information" can be any data or information that can be used to determine the presence of a user, and/or to identify and/or authenticate such a user. As such, presence information can include raw image, video, or audio data, analyzed data (e.g., video or image data to which preliminary facial recognition procedures, such as feature extraction, have been employed, as well as verification of audio self-identification or verification of audio challenge/response information), the results of such analysis, and even

the end result of the detection process—i.e., a notification that a user is present and/or an identification of the user.)

Detection of a user's presence can also be detected via proximity of a PDD and/or a video calling device to another device. For example, if a user's mobile phone, tablet, or PC is near the PDD and/or the ICD, that person is automatically detected. In some instances, a unique device identifier for each of a user's device might have previously been associated with the user's profile in a cloud database or the like (i.e., making the user's devices "known devices"), and detection of such unique device identifiers might serve as a basis for identifying the user, or might streamline the identification process by verifying whether the person with the device owned by or associated with the known device is the user or simply someone in possession of the device(s) (whether lawful or unlawful). Such verification might comprise one or more of facial recognition, voice recognition, audio challenge/response verification, biometric analysis, or the like. In some cases, audio challenge/response verification might include analysis of sub-vocal responses from the person challenged, to prevent undesired casual overhearing of audio passwords, audio keyphrases, or the like. In some instances, biometric analysis might include analysis of any suitable biometric (aside from facial and voice recognition) selected from a group consisting of fingerprint, iris, pupil, height, unique scar(s), other unique physical characteristics, and/or any combination of these biometrics. To capture biometric information such as fingerprints, iris, pupil, height, scar, or other unique physical characteristics, which might be image-based biometrics (which might be captured by a high resolution video capture device of the PDD and/or the ICD), the PDD and/or the ICD might prompt the person being identified to position himself or herself so that his or her fingerprints, iris, pupil, full body, scar, or other unique physical characteristics, respectively, are appropriately facing the video capture device of the PDD and/or the ICD.

In some embodiments, with detection of known devices and with automatic detection/identification processes being enabled, it may be possible for the system to identify persons not normally associated with a known device being in possession of the known device. In such a case, the system might notify the original user (via e-mail or other forms of communication indicated in the user's profile, or the like) of the situation. In some instances, the user might indicate that the unknown person does have authority or permission to use, or be in possession of, the user's device. In other cases, where the user indicates that the user does not have authority or permission to use the device, the user may be given options to proceed, including, without limitation, options to lock data, options to lock device functions, options to activate location tracking (including, without limitation, global positioning system ("GPS"), global navigation satellite system ("GNSS"), etc.) of the device (in case the system loses track of the device; e.g., in the case the device moves outside the range of the system's sensor/detection/communications systems), options to contact the unknown person, options to activate speakers to emit sirens, options to activate displays or lights (e.g., light emitting diodes ("LEDs"), organic LEDs ("OLEDs"), liquid crystal displays ("LCDs"), etc.), and/or options to notify authorities (e.g., police or other law enforcement personnel) of the situation and/or the location of the device (e.g., GPS coordinates, or the like), etc.

Additionally and/or alternatively, proximity detection can be done using GNSS location tracking functionality, which can be found in many electronic devices and authenticating the user when the secondary device is within a predefined distance of the PDD and/or ICD. Proximity detection can also

be done wirelessly via Bluetooth or WiFi. With respect to Bluetooth, if the secondary device pairs with the PDD and/or the ICD, the user can be considered detected. With respect to WiFi, one approach could be to see if the secondary device associates with the same WiFi access point that the PDD and/or the ICD is connected to. Another approach to proximity detection is the use of near-field communications ("NFC") commonly found in many electronic devices. When the secondary device is within range of the PDD and/or ICD, a NFC detector can be used to determine that the user is in the room. From these examples, a skilled reader should appreciate that many different techniques can be used to detect presence based on device proximity.

In some embodiments, detection of an individual can be fully automatic and might (in some instances) require no user interaction. For example, the system can characterize an individual's facial features (and/or unique physical characteristics or other biometrics) automatically, detect the presence of a secondary device, characterize an individual's voice print automatically, etc. Several detection methods can be used in combination to reduce errors in the detection process. For example, if the system detects a person in the room and first identifies that person's facial features, it can then prompt them for voice (e.g., "Bob, is that you?"). Once the user's voice is captured, that audio sample can be compared against the stored voice characteristics for that user, to reduce false detection. Another approach for the second step may be to prompt the user to speak a PIN or password to be compared against what is stored in the user profile. Using this approach, the characteristics of the speech (e.g., user's voice, cadence, syntax, diction) and the content of the speech (e.g., a PIN or password) can be jointly used to reduce false detections. To prevent eavesdropping of passwords or PINS, the audio capture device might be configured to capture subvocalizations of the passwords or PINS, for analysis. Alternatively and/or additionally, the system can prompt the user to position his or her body so as to allow the video capture device to face one or more of the user's fingers (e.g., for fingerprint analysis), the user's eyes (e.g., for iris and/or pupil analysis), the user's full body (e.g., for height analysis), portions of the user's body (e.g., for analysis of scars or other unique physical characteristics, or the like), etc.

In some embodiments, physical geography can be used as a metric in detection to reduce the possibility of errors. For example, if a user is known to use the system in Dallas, Tex., and then is detected in Madrid, Spain, the system can weigh detection in Spain lower than detection in Dallas. Additionally, if the user is detected in Spain, a secondary authentication method may optionally be invoked to reduce false detection. According to some embodiments, in the case that the system has access to profile or other personal information of the user such as communications, calendar items, contacts list, travel/itinerary information, or the like that might indicate that the user might be visiting a friend or relative in Spain having a similar PDD and/or ICD linked to a common network or cloud server, the system might determine that the user is or will be in Spain. In such a case, the user's profiles, media content, or the like (or access thereto) might be sent to the friend's or relative's device in Spain or to a local data center or the like to allow the user to access the user's own content or profiles on the friend's or relative's device during the visit; in particular embodiments, the user's profiles might include access and control information for remotely accessing and controlling the user's ICDs over a network, while the user's content might include image data and/or video data captured by the user's ICDs (either in raw or processed form). After the scheduled visit, it may be determined using any combination

11

of the user's personal information, the user's devices (including the user's PDD and/or ICD, mobile devices, etc.), and/or the friend's or relative's device whether the user has left the friend's or relative's location (in this example, Spain). If so determined, the content and profiles (or access thereto, as the case may be) might be removed from the friend's or relative's device (and/or from the data center or the like that is local to said device).

In particular embodiments, a PDD and/or a video calling device can also be connected to a network, such as the Internet. In such a scenario, the database of user profiles, including identifiable facial and/or voice characteristics, as well as other identifying information (e.g., passwords, identifying information for other devices owned by the user, etc.), can be stored on servers located in the cloud, i.e., on the network or in a distributed computing system available over the network. In some cases, the distributed computing system might comprise a plurality of PDDs and/or a plurality of ICDs in communication with each other either directly or indirectly over the network. The distributed computing system, in some instances, might comprise one or more central cloud servers linking the plurality of PDDs and/or the plurality of ICDs and controlling the distribution and redundant storage of media content, access to content, user profiles, user data, and/or the like. When an individual's facial features are detected by a PDD and/or a video calling device, those features (and/or an image captured by the PDD and/or the ICD) can be sent to a server on the network. The server then can compare the identifiable facial features against the database of user profiles. If a match is found, then the server might inform the device of the identity of the user and/or might send a user profile for the user to the device.

User profiles, including facial characteristics, can be stored both locally on the device and on a server located in the cloud. When using both device-based and cloud-based databases, user identification can be performed by first checking the local database to see if there is a match, and if there is no local match, then checking the cloud-based database. The advantage of this approach is that it is faster for user identification in the case where the user profile is contained in the local database. In some embodiments, the database on the device can be configured to stay synchronized with the database in the cloud. For example, if a change is made to a user profile on the device, that change can be sent to the server and reflected on the database in the cloud. Similarly, if a change is made to the user profile in the cloud-based database, that change can be reflected on the device database.

Matching presence information or identifying information with an individual having a user profile can be a form of authentication in some embodiments. User profiles can also contain information necessary for many authentication mechanisms. Such information may include challenge/response pairs (such as username and password combinations, security question/pass phrase combinations, or the like), facial recognition profiles, voice recognition profiles, and/or other biometric information, such as fingerprints, etc. An individual may be authenticated using any combination of such techniques.

In some cases, the system can also determine when a user is no longer present. Merely by way of example, a PDD and/or a video calling device might continually (or periodically) monitor for the user's presence. For instance, in the case of facial recognition, the device can continually check to detect whether a captured image includes the user's face. With voice recognition, after a period of inactivity, the device might prompt the user if they are there (e.g., "Bob, are you still there?").

12

According to some embodiments, user profiles can work across heterogeneous networks. Not all user devices need to be the same. Some user devices might be PDDs and/or ICDs. Other user devices might be computers, tablets, mobile phones, etc. Each can use any appropriate method (based on device capabilities) to determine the presence of, identify, and/or authenticate the user of the device with a user profile.

In an aspect, this automated presence detection can be used to provide user information (e.g., content or services) to an identified user. With a PDD and/or a video calling device, when a user enters the room, and the camera sensors detect that user's facial features (or other biometric features) and authenticates the individual, the content associated with that user profile (including, without limitation, profile information for handling video mail, profile information for remotely accessing recorded video mail or video mail data, and/or the like) can automatically become available to that individual. Additionally, with the cloud-based authentication approach described herein, that user's content and/or profiles can become available on any device. More specifically, if a user is identified by another PDD and/or video calling device, then his or her content (e.g., video mail or video mail data captured by the user's video calling device(s) or a video calling device(s) associated with another user, either in raw or processed form, and/or the like) becomes available to him or her even if the PDD and/or video calling device that he or she is in front of is not the user's own device. This functionality allows a new paradigm in which the user's content and/or profiles follow the user automatically. Similarly, when upgrading PDDs and/or video calling devices, detection, identification, and authentication of the user on the new device can allow automatic and easy porting of the user's content and/or profiles to the new device, allowing for an ultimate type of "plug-and-play" functionality, especially if the profiles include information on configurations and settings of the user devices (and interconnections with other devices).

PDDs and/or video calling devices also are capable of handling, transmitting, and/or distributing image captured content, which can include, but is not limited to, video mail and/or video mail data captured or recorded by the video calling devices. In some cases, the video mail and/or video mail data might be raw data, while in other cases they might be post-processed data. Video mail and/or video mail data can be stored on servers in the cloud, on PDDs/video calling devices in the cloud, and/or locally on a particular user device. When accessing video mail and/or video mail data from another device, the first PDD and/or video calling device that has the video mail and/or video mail data stored thereon needs to serve the video mail and/or video mail data to the new device that the user is using. In order to do this, the new PDD and/or video calling device might need to get a list of video mail and/or video mail data that is stored on the first PDD and/or video calling device. This can, in some embodiments, be facilitated via a server that is in the cloud that all PDDs and/or video calling devices are always or mostly connected to. The server can communicate with all PDDs and/or video calling devices and help send messages between PDDs and/or video calling devices. When a user is authenticated with a new PDD and/or video calling device, the new device can request the list of video mail and/or video mail data from the first device. If the user requests video mail and/or video mail data from the new device, then the first PDD and/or video calling device (or the other user device) can serve the video mail and/or video mail data to the new device. This can be done either directly in a peer-to-peer fashion or can be facilitated by

the server. In some embodiments, this communication can be accomplished by using protocols such as XMPP, SIP, TCP/IP, RTP, UDP, etc.

As discussed above, identification and authentication of a user by a PDD (whether or not associated with or owned by the user) can provide the user with remote access and control of the user's video calling device(s) over a network (e.g., by porting the user's profiles associated with remote access and control of the user's video calling device(s), and/or the like to the current PDD in front of which the user is located). This functionality allows the user to remotely access video mail and/or video mail data, to remotely access and modify settings for recording, post-processing, and accessing video mail and/or video mail data, and to remotely record a video or audio message prompting a missed video caller to leave a video mail message.

Master Account

Some embodiments employ a master account for access to a video calling device. In an aspect, a master account can be created on a per user basis. This master account might serve as the top-level identifier for a particular user. The master account is used to manage, control, and monitor a user's camera(s). Additionally, the master account can be used to control any account or device level services that are available.

For example, an email account and password can be used as a master account to manage a user's settings for handling, recording, post-processing, and/or accessing video mail and/or video mail data.

Device Association

For proper management and control of a video calling device, some embodiments provide the ability to reliably associate a video calling device with a master account (i.e., assign the video calling device to the master account). When a video calling device is associated with an account, then it can be managed and controlled from within the master account. Association ensures that a video calling device is being controlled by the appropriate user and not an unauthorized user.

A video calling device may be associated with a particular master account at the time of the device setup. During device setup, the user is prompted to enter a master account and password. When doing so, a secure communications channel may be opened up between video calling device and servers. Then, a unique and difficult to guess key can be sent from the device to the server. Servers that have a master list of all keys then can associate that particular device, via its serial number, to a particular master account. A feature of this approach is that a user only needs to enter a password at the time of device setup. The user never needs to enter a password again, and in fact, passwords do not need to be stored on the device at all, making them very secure.

Device Management and Remote Configuration

Once a device has been associated with a master account, it may be managed from the master account via an interface such as a web interface, in accordance with some embodiments. The communication link between the device and server may, in some cases, be always encrypted and authenticated. This ensures that messages between device and server are secure and ensures that the device knows it is communicating with the server on behalf of the appropriate master account. Once the secure and authenticated link is established, devices can connect to the server and are able to send and receive commands.

The device and server can have a common set of command codes and responses. Servers can send commands down to the camera(s) to enact specific behavior. For example, the server can send remote configuration commands. These commands

can be items such as changing the device address, changing the nickname that is associated with the device, changing the avatar image associated with the device. In addition to configuration, the commands can be used to enact specific behavior on the device, such as running network tests, or taking a live image(s) from the video calling device. New commands and features can be added by extending the set of command codes on the device and server.

Video Mail Capture, Processing, and Distribution

Certain embodiments provide tools to address the problem of a caller being able to leave a video mail for someone the caller is calling (i.e., a callee), when the callee is not able to take the video call. Some such embodiments are interoperable and do not require the caller (i.e., the person leaving the video mail) to have the same video calling device as the callee (i.e., the person for whom the message is left). In fact, any device (or software application) that interoperates with a video calling device in accordance with certain embodiments (i.e., can engage in a video call with such a device) is able to leave video mails for a callee who uses that device. U.S. patent application Ser. No. 12/581,185 (issued as U.S. Pat. No. 8,144,182) (the "'182 patent," the entire disclosure of which is hereby incorporated by reference for all purposes) discloses some exemplary video calling devices (also referred to in the '182 patent as video communication devices or VCDs) that can be used with embodiments disclosed herein. The PDD and/or ICD described above can also be used as a video calling device, in accordance with various embodiments. The '263 application (already incorporated by reference) discloses systems for capturing and processing video, including remote control over a video or image capture device. Embodiments disclosed herein can be employed in the environment disclosed in the '263 application and/or in conjunction with the techniques described in the '263 application, and/or such embodiments can be employed and/or be used in conjunction with video calling devices described in the '182 patent.

Merely by way of example, the '263 application describes networked systems (including cloud-based systems) for accessing a video calling device or other recording device, and/or for storing and/or processing images/video obtained by such a device. Such systems can be employed to provide the video mail services described herein.

Some embodiments implement video mail features by way of an actual video call. From a technical perspective, the calling device enters an actual video call with the callee's video calling device, just as it would if the callee answered the video call. This feature can allow the callee's video calling device to record video mail not just from another similar device, but from any device and/or software application (which might be executed on tablets, mobile phones, personal computers ("PCs"), and/or other user devices, etc.) that can engage in a video call with the video calling device (which can be implemented by the image capture device described in the '263 application and/or the video communication devices disclosed in the '182 patent).

Once a videomail is left, the callee's video calling device might upload the components of the videomail to the cloud (e.g., the cloud environment described in the '263 application). Once in the cloud, the audio and video can be post processed into any desired format (including, as one specific example, a format that is viewable by a web browser). Once the post-processing is complete, the owner of the video calling device that received the voicemail (i.e., the user or callee) can be notified of the new videomail.

A number of different notifications can be provided. Merely by way of example, a notification might take the form of an e-mail that is automatically generated and sent to the

15

user's or callee's e-mail address (e.g., as registered with the video calling provider). The e-mail might contain a link to the videomail itself. In this manner, the videomail can be viewed on any device that is capable of accessing the link. This means that the videomail can be viewed on any device that is capable of viewing the video itself (e.g., PC, tablet device, smart-
phone, etc.). Additionally, the provider can store a user's videomails in the cloud, and presents the list of videomails a user has using the provider's web portal interface. A user can log into the portal using a web browser and see all the videomails that have been left for him or her. Videomails can also be deleted as well.

In an exemplary (but non-limiting) embodiment, the following workflow can be used to implement videomail:

(1) The video calling device is configured for videomails. In an aspect, the device can be configured to optionally answer videomails (i.e., such functionality can be turned on or off). Other behavior that can be configured is the amount of time to wait before triggering the device to record a videomail. Such configuration can be established, set, or modified with the user interface of the device itself, with the web portal interface, and/or using any other suitable technique.

(2) A caller initiates a video call to the video calling device.

(3) If the video calling device is configured to record video mails, then at the appropriate time, it will automatically answer the video call. From a technical perspective, the calling device and the video calling device are now in a video call.

(4) Rather than sending video and audio from its camera and microphone as it would in a normal video call, the video calling device will send pre-recorded graphics and audio. The video calling device can start by sending a graphic that indicates that the receiving party is not available and that the caller may leave a videomail. For example, language can include "The person you called is not available. At the tone, please leave a videomail." From an audio perspective, a pre-recorded message with similar language can be sent. Once this message is sent, then an audible tone might be sent to the calling party. This tone can be used to indicate to the caller that he or she may begin recording a videomail. Additionally, after the tone, the video calling device transmits a graphic with language such as, "Currently recording videomail," to visually indicate to the caller that his or her message is being recorded.

(5) Once the calling party begins transmitting audio and video, the video calling device begins recording the audio and video streams to the local disk. To avoid visible artifacts in the recorded videomail, the video calling device begins recording video when an Instantaneous Decoder Refresh ("IDR") video frame is received. If one is not received, video calling device requests one from the caller. In fact, the audible tone in step (4) is not played until an IDR frame is received. This ensures that the caller does not begin speaking until artifact free video can be recorded.

(6) In typical video calls, audio and video are transmitted as independent streams, which are decoded and synchronized by the receiving device. Synchronization must also be preserved on the playout device, which may not be a video calling device, but might be a PC, a smartphone, a tablet, and/or the like. There are many ways to perform decoding and/or synchronization, but one possible approach is as follows:

The video calling device records all incoming video to the local disk, without decoding the incoming video.

The video calling device decodes all audio from the calling party. In doing so, the video calling device runs all of its

16

error concealment and synchronization algorithms. Then, the video calling device records the audio to the local disk.

The video calling device runs its audio and video synchronization algorithms and records a "timecode" file to the disk. The timecode file indicates when each video frame should be displayed. There are other variations of this; however, in this implementation, audio and video are both recorded to the local disk and a timecode file is also recorded that can help a post processor synchronize audio and video.

(7) Audio and video are recorded for a pre-determined amount of time (e.g., 2 minutes), or until the local disk is full.

(8) The audio, video, and timecode files are uploaded to the cloud for post-processing. Additionally, the sampling rate of the audio is also passed to the cloud. The purpose of the post-processing is to convert these elements into a video file that can be played on any device (including, but not limited to, PC, tablet, mobile phone, and/or the like).

(9) The raw elements are post-processed in the cloud. This may be performed to avoid heavy processing performed by the video calling device itself. The post-processing algorithms might perform some or all of the following operations:

Scale the video to a consistent resolution. The recorded video can have multiple resolutions in it as this typically can vary in video calls. However, many tools used to view video on PCs, tablets, phones, and/or the like cannot handle varying resolution. Thus, a single resolution makes the video playable on many devices.

Mix the audio and video together. The mixing also uses the timecode file that is uploaded to determine when to display the video frames. The audio is also mixed at the correct sampling rate.

Add a visible watermark to the video for marketing purposes.

Generate a resulting video file having a format that can be played on many systems, including, without limitation, MP4 format or the like.

(10) Once the video has been generated, an e-mail can be sent to the owner of the called video calling device. The e-mail might contain a link (e.g., a URL) to the video that is live. This allows the video calling device owner to view the videomail wherever he or she is. The device owner does not need to be near his or her device. A sample e-mail that is generated is shown in FIG. 6A. Alternatively, or additionally, the e-mail might contain an attachment comprising the video, and/or might have the video embedded in the e-mail.

(11) Additionally, the videomail may be presented to the users in their video calling provider's web portal interface. The web interface, which displays who the videomail is from and shows the sender's picture, might show the length of the videomail as well. The web interface might also show all videomails that the user has received and might allow the user to delete the videomails as well. An example of a web interface is shown, e.g., in FIG. 6B.

Exemplary Embodiments

FIGS. 1-8 illustrate exemplary embodiments that can provide some or all of the features described above. The methods, systems, and apparatuses illustrated by FIGS. 1-8 may refer to examples of different embodiments that include various components and steps, which can be considered alternatives or which can be used in conjunction with one another in the various embodiments. The description of the illustrated methods, systems, and apparatuses shown in FIGS. 1-8 is provided

17

for purposes of illustration and should not be considered to limit the scope of the different embodiments.

FIG. 1 illustrates a functional diagram of a system 100 for controlling one or more PDDs and/or one or more video calling devices (labeled user devices 105 in FIG. 1 for ease of illustration, but described herein as PDDs or video calling devices, each of which can be considered a type of user device). The skilled reader should note that the arrangement of the components illustrated in FIG. 1 is functional in nature, and that various embodiments can employ a variety of different structural architectures. Merely by way of example, one exemplary, generalized architecture for the system 100 is described below with respect to FIG. 8, but any number of suitable hardware arrangements can be employed in accordance with different embodiments.

A video calling device 105 or a PDD 105 can be any device that is capable of communicating with a control server 110 over a network 115 and can provide any of a variety of types of video communication functionality. Merely by way of example, in some aspects, a video calling device 105 or a PDD 105 can be capable of providing pass through video/audio to a display device (and/or audio playback device) from another source (such as a local content source), and/or overlaying such video/audio with additional content generated or received by the video calling device 105 or the PDD 105. In other aspects, a video calling device 105 or a PDD 105 can comprise one or more sensors (e.g., digital still cameras, video cameras, webcams, security cameras, microphones, infrared sensors, touch sensors, and/or the like), and/or can be capable, using data acquired by such sensors, of sensing the presence of a user, identifying a user, and/or receiving user input from a user; further, a video calling device 105 or a PDD 105 can be capable of performing some or all of the other functions described herein and/or in the Related Applications. Hence, in various embodiments, a video calling device 105 or a PDD 105 can be embodied by a video calling device, such as any of the VCDs described in the '182 patent, a video game console, a streaming media player, to name a few non-limiting examples.

In one aspect of certain embodiments, as described more fully with respect to FIG. 5 below, a video calling device 105 or a PDD 105 can be placed functionally inline between a local content source and a display device. A local content source can be any device that provides an audio or video stream to a display device and thus can include, without limitation, a cable or satellite set-top box ("STB"), an Internet Protocol television ("IPTV") STB, devices that generate video and/or audio, and/or acquire video and/or audio from other sources, such as the Internet, and provide that video/audio to a display device; hence, a local content source can include devices such as a video game console, a Roku® streaming media player, an AppleTV®, and/or the like. When situated functionally inline between a local content source and a display device, the video calling device or the PDD can receive an audiovisual stream output from the local content source, modify that audiovisual stream in accordance with the methods described herein, in the '182 patent, and/or in the '279 application, and provide the (perhaps modified) audiovisual stream as input to the display device. It should be noted, however, that, in some cases, the functionality of a local content source can be incorporated within a video calling device or a PDD, and/or the functionality of a video calling device or a PDD can be incorporated within a local content source; further, it should be appreciated that a video calling device or a PDD (which might or might not include local content source functionality) can be disposed inline with one or more other local content sources or one or more

18

other video calling devices/PDDs. Hence, for example, a video calling device or a PDD with some local content source functionality (such as a video game console) might be disposed inline between one or more other local content sources or one or more other video calling devices/PDDs (such as a cable STB, satellite STB, IPTV STB, and/or a streaming media player) and a display device.

In an aspect of some embodiments, the system can include a software client that can be installed on a computing device (e.g., a laptop computer, wireless phone, tablet computer, etc.) that has a built-in camera and/or has a camera attached (e.g., a USB webcam). This client can act as an interface to allow remote control of the built-in and/or attached camera on the computing device. In some embodiments, the computing device might have a built-in microphone(s) and/or has a microphone(s) attached (e.g., a table-top microphone, a wall-mounted microphone, and/or a microphone removably mountable on a television, on the video calling device, on the PDD, and/or on some other suitable user device, or the like). The software client can alternatively and/or additionally act as an interface to allow remote control of the built-in and/or attached microphone on the computing device. In some cases, the camera and/or microphone can be automatically or autonomously controlled to obtain optimal video and/or audio input. Remote control of the video calling device and/or PDD is described in detail in the '263 application (already incorporated herein).

The system 100 can further include a control server 110, which can have any suitable hardware configuration, and an example of one such configuration is described below in relation to FIG. 8. In one aspect, the control server 110 is a computer that is capable of receiving user input via a user interface 120 and/or performing operations for utilizing the video calling device(s) 105 and/or the PDD(s) 105 to receive video calls, to determine that a user or callee is unavailable to receive a video call, to prompt a caller to leave a videomail message, to record the videomail message, to upload the videomail message for post-processing, to notify the user or callee about the videomail message, to enable the user or callee to remotely access the user's master account, user preferences, and/or the videomail message, and/or the like, for example as described in further detail below. Merely by way of example, the control server 110 can detect user presence, identify/authenticate users, and/or enable the user to remotely access the user's master account, user preferences, the videomail message, and/or the like. In other cases, the control server 110 can receive and/or store user input and/or user preferences that can specify whether and how presence information should be used, whether and how the user's video calling device(s) and/or PDD(s) may be used in the distributed infrastructure, whether and how the user's content and profiles should be handled under certain situations, and/or the like.

For example, preferences might specify which account information, content, profile information, personal communications (e.g., videomail, etc.), and/or the like should be delivered to a user when present at a device not owned by the user, whether presence information should be collected for that user at all (and/or where such information should be collected); for example, a user might specify that his presence should only be monitored in selected locations or from selected devices, and the control server 110 might remove that user's profile from the search universe when provided with presence information from a device not at the selected location or from a device other than one of the selected devices. More generally, the user preference can include any types of parameters related to collecting presence informa-

19

tion, using presence information, and/or serving content/information (including, without limitation, user account information, user content, user profile information, user's personal communications (e.g., videomail, etc.), and/or the like). These preferences might be stored in a user profile at the control server 110, which might also include other user-specific information, such as the user's normal location(s), identifying information (such as MAC address, etc.) of other user devices owned by or associated with the user, lists of or links to content owned by the user, lists of or links to videomail messages addressed to the user, and/or the like.

In some embodiments, user preferences might specify how the user would like his or her user devices to participate (or not) in a distributed infrastructure arrangement. For instance, the user preferences might include, without limitation, preferences indicating whether or not to allow a user device owned by the user to be used for distributed infrastructure; preferences indicating what type of software applications, customer data, and/or media content (of other user device users and/or subscribers of a cloud service) are permitted to be hosted on a user device owned by the user; and/or preferences indicating amount of resources of a user device to dedicate to the distributed infrastructure; etc. In some embodiments, in addition to indicating how a user's user device may be used in distributed infrastructure implementation, user preferences might allow a user to indicate how the user's own applications, data, and/or media content may be hosted on other users' user devices. For example, the user might be given the option to encrypt any and/or all personal data, any and/or all personal applications, any and/or all files or lists indicating which media content are associated with the user, and/or any and/or all files or lists pertaining to videomail messages that are addressed to the user (including the videomail messages themselves). Common media content (which might include popular media content, or any other media content) may remain unencrypted for common usage by any number of users on any number of user devices, subject only to any subscription, rental, or purchase restrictions on the particular media content as associated with any user and/or any user device. On the other hand, the user's personal communications (including, e.g., videomail messages and/or the like) may be encrypted.

In some examples, the user might indicate that her user device may be used for distributed processing, but not distributed cloud-based data storage, or vice versa. Alternatively, the user might indicate that her user device may be used for both distributed processing and distributed cloud-based data storage. In some embodiments, the user might allow the hosting, on his or her user device, of at least portions of software applications that are published by known and reputable software companies or published by companies on behalf of governmental agencies, or the like, while blocking hosting of software applications associated with marketing, spam, data mining, and/or potential copyright violations, etc. These and other preferences related to distributed infrastructure functionality are described in greater detail in the '360 application (which is already incorporated herein by reference).

With respect to video mail capture, processing, and distribution functionality, user preferences might include, without limitation, preferences indicating one or more video calling devices to associate with a master account, preferences indicating under what conditions the one or more video calling device(s) should prompt callers to leave videomail messages, preferences indicating whether presence detection functionality (as described in detail in the '279 application) should or should not be enabled in a particular one(s) of the one or more video calling device(s), preferences associated with record-

20

ing, notifying, and distributing videomail messages, preferences indicating whether or not (and under what conditions) videomail messages should be post-processed (and how), preferences indicating how the user may access the user's master account, user profiles, user preferences, videomail messages, and/or the like.

The control server 110 can provide a user interface (which can be used by users of the video calling devices 105 and/or the PDDs 105, and/or the like). The control server 110 might also provide machine-to-machine interfaces, such as application programming interfaces ("APIs"), data exchange protocols, and the like, which can allow for automated communications with the video calling devices 105 and/or the PDDs 105, etc. In one aspect, the control server 110 might be in communication with a web server 125 and/or might incorporate the web server 125, which can provide the user interface, e.g., over the network to a user computer (not shown in FIG. 1) and/or a machine-to-machine interface. In another aspect, the control server 110 might provide such interfaces directly without need for a web server 125. Under either configuration, the control server 110 provides the user interface 120, as that phrase is used in this document. In some cases, some or all of the functionality of the control server 110 might be implemented by the video calling device 105 and/or the PDD 105 itself.

In an aspect, the user interface 120 allows users to interact with the control server 110, and by extension, the video calling devices 105 and/or the PDDs 105. A variety of user interfaces may be provided in accordance with various embodiments, including, without limitation, graphical user interfaces that display, for a user, display fields on display screens for providing information to the user and/or receiving user input from a user. Example graphical user interfaces are shown in FIG. 6 as described below.

Merely by way of example, in some embodiments, the control server 110 may be configured to communicate with a user computer (not shown in FIG. 1) via a dedicated application running on the user computer; in this situation, the user interface 120 might be displayed by the user computer based on data and/or instructions provided by the control server 110. In this situation, providing the user interface might comprise providing instructions and/or data to cause the user computer to display the user interface. In other embodiments, the user interface may be provided from a web site, e.g., by providing a set of one or more web pages, which might be displayed in a web browser running on the user computer and/or might be served by the web server 125. As noted above, in various embodiments, the control system 110 might comprise the web server and/or be in communication with the web server 125, such that the control server 110 provides data to the web server 125 to be incorporated in web pages served by the web server 125 for reception and/or display by a browser at the user computer.

The network 115, specific examples of which are described below with regard to FIG. 8, can be any network, wired or wireless, that is capable of providing communication between the control server 110 and the video calling devices 105 and/or the PDDs 105, and/or of providing communication between the control server 110 (and/or the web server 125) and a user computer. In a specific embodiment, the network 115 can comprise the Internet, and/or any Internet service provider ("ISP") access networks that provide Internet access to the control server 110, the user computer, and/or the video calling devices 105 and/or the PDDs 105.

In some embodiments, the system 100 can include a cloud storage system 130, which can be used, as described in further detail below, to store advertisements, presence information,

21

images, video, and/or videomail messages that are captured and uploaded by the video calling devices **105** and/or the PDDs **105**, and/or the like. In some cases, the cloud storage system **130** might be a proprietary system operated by an operator of the control server **110**. In other cases, the cloud storage system **130** might be operated by a third party provider, such as one of the many providers of commercially available cloud services. In yet a further embodiment, the cloud storage system **130** might be implemented by using resources (e.g., compute, memory, storage network, etc.) shared by a plurality of video calling devices, and/or by a plurality of PDDs, that are distributed among various users of the system. Merely by way of example, as described in further detail below and in the '360 application (already incorporated by reference herein), a plurality of user video calling devices and/or PDDs might each have some dedicated resources (such as a storage partition), which are dedicated for use by the system, and/or some ad hoc resources (such as network bandwidth, memory, compute resources, etc.) that are available to the system when not in use by a user. Such resources can be used as cloud storage and/or can be used to provide a distributed, cloud-like platform on which a control server can run as a virtual machine, cloud container, and/or the like.

According to some embodiments, video calling device **105** might comprise a first video input interface to receive first video input from a first local content source (which in some embodiments can include a STB and/or the like) and a first audio input interface to receive first audio input from the first local content source. Video calling device **105** might further comprise a first video output interface to provide first video output to a first video display device and a first audio output interface to provide first audio output to a first audio receiver. In some cases, the first video display device and the first audio receiver might be embodied in the same device (e.g., a TV with built-in speaker system, or the like). With the input and output interfaces, video calling device **105** might provide pass-through capability for video and/or audio between the first local content source and the first display device. In some instances, high-definition multimedia interface ("HDMI") cables or other suitable HD signal cables may be used to provide the interconnections for the pass-through. Video calling device **105** may, in some cases, comprise a first video capture device to capture at least one of first image data or first video data and a first audio capture device to capture first audio data. Video calling device **105** may also comprise a first network interface, at least one first processor, and a first storage medium in communication with the at least one first processor.

In some aspects, a plurality of video calling devices **105** might be communicatively coupled together in a network (e.g., network **115**), each video calling device being located in one of a plurality of customer premises. For implementing distributed infrastructure for cloud computing, cloud-based application hosting, and/or cloud-based data storage, a computer might establish one or more video calling devices **105** of the plurality of video calling devices **105** as distributed infrastructure elements and might provide at least one of one or more software applications, customer data, and/or media content to the one or more video calling devices **105** for hosting on the one or more video calling devices **105**. These and other functionalities of the video calling devices related to distributed infrastructure are described in greater detail in the '360 application (already incorporated by reference herein).

Merely by way of example, in some aspects, a user can remotely access one or more video calling devices **105** and/or remotely access at least one of the user's master account, the user's user preference, the user's profiles, any videomail mes-

22

sages addressed to the user, and/or the like over a network. For example, in a web-based implementation, a user could log into the user's master account by accessing a website hosted on a web server (e.g., web server **125**, which might be hosted on a cloud server, hosted on distributed PDDs, hosted on distributed video calling devices, and/or the like) and entering commands into a user interface (e.g., user interface **120**) associated with remotely accessing the user's video calling device(s) **105** and/or associated with remotely accessing at least one of the user's master account, the user's user preference, the user's profiles, any videomail messages addressed to the user, and/or the like. In some instances, the user might access and interact with the user interface over the network (e.g., network **115**) by using a user computer selected from a group consisting of a laptop computer, a desktop computer, a tablet computer, a smart phone, a mobile phone, a portable computing device, and/or the like. In an application-based (or "app-based") implementation, the user might interact with a software application (or "app") running on the user's user device, which might include, without limitation, a laptop computer, a desktop computer, a tablet computer, a smart phone, a mobile phone, a portable computing device, and/or the like. The app might include another user interface (similar to the web-based user interface) that might allow for access of the user's video calling device(s) (or any paired video calling device(s)) over the network (e.g., network **115**) and/or that might allow for access to at least one of the user's master account, the user's user preference, the user's profiles, any videomail messages addressed to the user, and/or the like.

In some embodiments, access of one or more video calling device(s) and/or access to at least one of the user's master account, the user's user preference, the user's profiles, any videomail messages addressed to the user, and/or the like may be permitted in response to identification and/or authentication of the user by a PDD ("PDD"), as described in detail herein and in the '279 application. In some embodiments, a PDD **105** might comprise a second video input interface to receive second video input from a second local content source (which, in some embodiments, might include a STB and/or the like) and a second audio input interface to receive second audio input from the second local content source. PDD **105** might further comprise a second video output interface to provide second video output to a second video display device and a second audio output interface to provide second audio output to a second audio receiver. In some cases (as with video calling device **105** above), the second video display device and the second audio receiver might be embodied in the same device (e.g., a TV with built-in speaker system, or the like). With the input and output interfaces, PDD **105** might provide pass-through capability for video and/or audio between the second local content source and the second display device. In some instances, high-definition multimedia interface ("HDMI") cables or other suitable HD signal cables may be used to provide the interconnections for the pass-through. PDD **105** may, in some cases, comprise a second video capture device to capture at least one of second image data or second video data, and a second audio capture device to capture second audio data. PDD **105** might also comprise a second network interface, at least one second processor, and a second storage medium in communication with the at least one second processor. Similar to the video calling devices **105**, a plurality of PDDs **105** may be communicatively coupled together in a network (e.g., network **115**), as distributed infrastructure elements for implementing distributed infrastructure for cloud computing, cloud-based application hosting, and/or cloud-based data storage.

23

Once a user has been automatically identified and/or authenticated by a user device having identification and/or authentication functionality (e.g., by a PDD as described herein or as described in the '279 application), regardless of whether or not the user is associated with (or owns) such user device, the user may be provided with access to the video calling device(s) over the network and/or remote access to at least one of the user's master account, the user's user preference, the user's profiles, any videomail messages addressed to the user, and/or the like. Such access (as discussed above) may be in the form of web-based user interfaces, app-based user interfaces, or other suitable user interfaces. Such user interfaces might be customized automatically based on the user preferences (i.e., based on the video mail capture, processing, and distribution user preferences discussed above). In some instances, the user interfaces might be configured to allow addition, modification, and/or deletion of such user preferences. According to some embodiments, the user interfaces might provide the user with options for uploading, locally storing, cloud storing, distributing/sharing, processing, and/or otherwise handling recorded videomail messages from the video calling device(s). Some of these options may be preselected (or established as default settings) in the user preferences. In some cases, processing of videomail messages from the video calling device(s) might include, without limitation, formatting, sharpening, and/or otherwise manipulating the videomail messages.

In some cases, the user device (e.g., PDD) might be configured to determine whether the user is no longer present. Based on such a determination, access to the video calling device(s) over the network, as well as access to at least one (if not all) of the user's master account, the user's user preference, the user's profiles, any videomail messages addressed to the user (whether in the raw or processed state), and/or the like, may be blocked. Blocking such access may include automatically logging out of the web-based or app-based user interface, or the like.

FIG. 2 illustrates a method 200 of enabling or implementing video mail capture, processing, and distribution, in accordance with one set of embodiments. While the techniques and procedures are depicted and/or described in a certain order for purposes of illustration, it should be appreciated that certain procedures may be reordered and/or omitted within the scope of various embodiments. Moreover, while the method illustrated by FIG. 2 can be implemented by (and, in some cases, are described below with respect to) the system 100 of FIG. 1 (or components thereof), such methods may also be implemented using any suitable hardware implementation. Similarly, while the system 100 of FIG. 1 (and/or components thereof) can operate according to the method illustrated by FIG. 2 (e.g., by executing instructions embodied on a computer readable medium), the system 100 can also operate according to other modes of operation and/or perform other suitable procedures.

At block 205, method 200 might comprise receiving, at a first video calling device associated with a user (or callee), a video call from a caller at a second video calling device. In some instances, the first video calling device and the second video calling device might be made by different manufacturers and/or might be of different models of calling device. Method 200 might, at block 210, comprise determining that the user is unable to answer the video call. In some instances, such a determination might be based at least in part on presence detection functionalities described herein that indicate the user is not present or near the first video calling device, or based at least in part on presence detection functionalities described herein that indicate the user is in a conversation

24

with someone else (e.g., based on voice identification, and/or the like). In some embodiments, such a determination might be based at least in part on current user settings or user status (indicating e.g., that the user is busy, away, or otherwise not to be disturbed, or the like).

Method 200 might further comprise prompting the caller to leave a videomail message, e.g., based at least in part on a determination that the user is unavailable to answer the video call (block 215). In some instances, the prompt might include a text, voice, and/or video message pre-recorded by the user prompting callers to leave videomail messages. At block 220, method 200 might comprise recording the videomail message from the video call. In some cases, recording the videomail message from the video call might comprise first establishing a video call connection with the caller and subsequently recording the videomail message. In other instances, recording the videomail message from the video call might comprise recording a video stream from the caller (i.e., data packet stream or the like from the caller), without first establishing a video call connection.

Method 200, at block 225, might comprise uploading, over a network, the videomail message to a server for post-processing. In some cases, uploading the videomail message might comprise uploading to a specified location on the network (which might be specified by the user, e.g., via the user interface, and/or might be specified by the system itself without user input). In some instances, the specified location might be a cloud storage system, such as that provided by Amazon Web Services™ and/or the like. In an aspect of some embodiments, the system can cause the video calling device(s) to upload the videomail message directly to the cloud environment, without transmitting the videomail message to any intermediary server (including the control server itself or any other device), preventing bottlenecks in the upload process. Merely by way of example, the control server might comprise a command including a uniform resource locator ("URL") pointing to a location in the cloud environment to which the videomail message should be uploaded.

In a particular set of embodiments, the system might segment the storage environment (whether a cloud storage environment or otherwise) into partitions (e.g., directories, etc.) that are assigned to particular master accounts and/or, within such partitions, subpartitions assigned to individual video calling devices assigned to those master accounts. Hence, the method might comprise storing the videomail message in a location assigned to that master account and/or video calling device(s). In a particular set of embodiments, the system might provide the master account with control over access to the uploaded videomail messages, e.g., by allowing the authenticated user to specify whether a given file or set of files should be available only to the user, to others specified by the user, or to the public. In any case, the system might assign a URL to the uploaded videomail message and/or might provide that URL to the user (e.g., via the user interface), so that the user can access the videomail messages at a later time, share the URL with others, and/or the like. The URL might be private (e.g., accessible only to the master account) or public (e.g., accessible to anyone, and in particular, to whom the user gives the URL).

At block 230, method 200 might comprise performing post-processing of the videomail message. In some embodiments, post-processing of the videomail message might comprise, without limitation, scaling video of the videomail message to a specified resolution, mixing audio and video of the videomail message by reference to a timecode, adding a visible watermark to the videomail message, formatting the videomail message as a video viewable by a web browser,

25

and/or the like. The specified resolution might include, but is not limited to, a resolution common to most, if not all, video playback devices, high-definition resolution, and/or the like). In some cases, the specified resolution might be a default resolution or a resolution set by the user in the preferences for videomail, or the like.

In some cases, prompting the caller to leave the videomail message (at block 215) and recording the videomail message (at block 220) might each be performed by the first video calling device associated with the user, while in other cases, prompting the caller to leave the videomail message (at block 215) and recording the videomail message (at block 220) might each be performed by the second video calling device associated with the caller. According to some embodiments, recording the videomail message (at block 220) might comprise recording a timecode file to a storage medium at one of the first video calling device or the second video calling device. The timecode file might indicate when each frame of video of the videomail message should be displayed. Recording the videomail message (at block 220) might further comprise synchronizing, at the one of the first video calling device or the second video calling device, audio and video from the videomail message, based at least in part on the recorded timecode file. In some instances, uploading the videomail message to the server (at block 225) might comprise uploading an audio file, a video file, and the timecode to the server.

At block 235, method 200 might comprise storing the post-processed videomail message either locally (i.e., on the one of the first video calling device or the second video calling device) or remotely over the network (i.e., at the server or at a database in communication with the server, or the like). Method 200 might further comprise providing a notification to the user regarding the videomail message (block 240). In some instances, the notification might comprise an e-mail message with a link to a formatted video comprising the videomail message. In some cases, a uniform resource locator ("URL") addressing the formatted video might be created, and the link might include the URL addressing the formatted video. According to some embodiments, the e-mail message might include an attachment comprising the videomail message. In some cases, the e-mail message might have the videomail message embedded in it.

Method 200, at block 245, might comprise receiving a request from the user to view the videomail message. In the case of the link to the videomail message, the request might comprise the user clicking on or otherwise following the link. In the case of the attached or embedded videomail message, the request might comprise the user interacting with the e-mail client to open the attachment. At block 250, in response to the request to view the videomail message, method 200 might comprise displaying the videomail message (e.g., on a display device of a user computing device associated with the user, and/or the like). In some embodiments, the videomail message might be displayed in a user interface, such as a pop-up window or in a main window, or in a user interface described with respect to FIGS. 3, 4, and 6 below. In the case of the link to the videomail message, pop-up window or the main window might be a window of a web-browser. For example, a web page that provides the user interface might include a frame, window, or applet that displays a videomail message uploaded from the video calling device(s). In a particular aspect, the server might obtain the videomail message from the location to which the video calling device(s) uploaded the videomail message, and/or the server (and/or web server) might insert into the web page an anchor that references the videomail message in another location (such as a location in a cloud storage system where the

26

videomail message was uploaded). In the case of the attached or embedded videomail message, the pop-up window or the main window might be a window of the e-mail client, a window of a local video playback client, and/or the like. In some aspects, the videomail message might be displayed within an e-mail message (particularly in the case of the embedded videomail message).

At block 255, method 200 might comprise receiving a request from the user to respond to a videomail message. Method 200, at block 260, might comprise enabling the user to respond to the videomail message, by initiating a video call request to the original caller who left the videomail message, by leaving a videomail message for the original caller (e.g., in the case that the original caller is presently unavailable to answer the video call), by initiating a voice or telephone call to the original caller, by sending an e-mail message to the original caller, by sending a text message to the original caller, and/or the like.

FIG. 3 illustrates a method 300 of enabling remote access to user preferences for videomail and enabling remote access to videomail, in accordance with one set of embodiments. While the techniques and procedures are depicted and/or described in a certain order for purposes of illustration, it should be appreciated that certain procedures may be reordered and/or omitted within the scope of various embodiments. Moreover, while the method illustrated by FIG. 3 can be implemented by (and, in some cases, are described below with respect to) the system 100 of FIG. 1 (or components thereof), such methods may also be implemented using any suitable hardware implementation. Similarly, while the system 100 of FIG. 1 (and/or components thereof) can operate according to the method illustrated by FIG. 3 (e.g., by executing instructions embodied on a computer readable medium), the system 100 can also operate according to other modes of operation and/or perform other suitable procedures.

Turning to FIG. 3, the method 300 might comprise registering a master account for a user (block 305). In accordance with various embodiments, registering a master account for a user can comprise a variety of operations. Merely by way of example, registering a master account can comprise creating a database entry for a particular user and/or assigning authentication credentials to that user; these credentials can be used to access the master account, as described in further detail below.

The method 300 can also include assigning one or more video calling devices to the master account (block 310). For instance, the user might identify any video calling devices that the user owns (or is otherwise associated with; e.g., members of the user's family might be associated with the devices owned by the user), and the system can assign those video calling devices to the user's master account. According to some embodiments, the user's master account might include any suitable number of sub-accounts. In one example, each member of the user's family might be associated with a sub-account linked with the master account. In some instances, the user (or some members of his or her family) might have a work/school sub-account and a home sub-account, the former being associated with profiles and/or media content appropriate for school or work, while the latter being associated with all, or all other, profiles and/or media content. In some embodiments, the master account and the plurality of sub-accounts might be organized as a hierarchy, with the master account (being at the top of the hierarchical structure) having full access to profiles and media content of each sub-account, the sub-accounts at the next level having access to profiles and/or media content of only those sub-accounts that the master account has given access to, and the sub-accounts

at lower levels having limited access to profiles and/or media content. For example, the user's master account might have access to all profiles and/or media content associated with the master account and the sub-accounts. The user can provide his or her spouse with a sub-account having the same access to profiles and/or media content, while providing limited access to profiles and/or media content to each of the user's children's sub-account(s). In some instances, the user and/or the user's spouse might impose limits on access to profiles and/or media content for each of their work sub-accounts.

In some cases, each video calling device might have an identifier, such as a hardware identifier, IP address, nickname, and/or the like, by which the system can address the video calling device, and assigning a video calling device to the master account can comprise associating that identifier with the master account. When a video calling device is assigned to a master account, the user of that account will be able to access, configure, and/or control the video calling device through the control server, for example as described in further detail below. In some cases, the user might own a plurality of video calling devices and might wish to control all of the video calling devices from a single master account. In an aspect, a user can identify such devices through a user interface to the control server.

In another aspect, as described briefly above, the assignment process can be simplified. When the user first configures a video calling device (usually locally, but perhaps over the network), the user can provide credentials to the video calling device that associate the device with the master account. Thereafter, the video calling device might be configured to communicate with the control server and identify itself using those credentials; at that point, the control server can assign the video calling device to the master account, and no credentials need to be stored on the video calling device from that point forward (other than perhaps the video calling device's own identifying information).

The method **300**, in the illustrated embodiment, might further comprise providing a user interface to allow interaction between the user and the control server (block **315**). For example, the user interface can be used to output information for a user, e.g., by displaying the information on a display device, printing information with a printer, playing audio through a speaker, etc.; the user interface can also function to receive input from a user, e.g., using standard input devices such as mice and other pointing devices, motion capture devices, touchpads and/or touchscreens, keyboards (e.g., numeric and/or alphabetic), microphones, etc. The procedures undertaken to provide a user interface, therefore, can vary depending on the nature of the implementation; in some cases, providing a user interface can comprise displaying the user interface on a display device; in other cases, however, in which the user interface is displayed on a device remote from the computer system (such as on a client computer, wireless device, etc.), providing the user interface might comprise formatting data for transmission to such a device and/or transmitting, receiving, and/or interpreting data that is used to create the user interface on the remote device. Alternatively and/or additionally, the user interface on a client computer (or any other appropriate user device) might be a web interface, in which the user interface is provided through one or more web pages that are served from a computer system (and/or a web server in communication with the computer system), and are received and displayed by a web browser on the client computer (or other capable user device). The web pages can display output from the computer system and receive input from the user (e.g., by using Web-based forms, via hyperlinks, electronic buttons, etc.). A variety of techniques can be

used to create these Web pages and/or display/receive information, such as JavaScript, Java applications or applets, dynamic Hypertext Markup Language ("HTML") and/or Asynchronous JavaScript and XML (or extensible markup language) ("AJAX") technologies, to name but a few examples.

In many cases, providing a user interface will comprise providing one or more display screens each of which includes one or more user interface elements. As used herein, the term "user interface element" (also described as a "user interface mechanism" or a "user interface device") means any text, image, or device that can be displayed on a display screen for providing information to a user and/or for receiving user input. Some such elements are commonly referred to as "widgets," and can include, without limitation, text, text boxes, text fields, tables and/or grids, menus, toolbars, charts, hyperlinks, buttons, lists, combo boxes, checkboxes, radio buttons, and/or the like. While any illustrated exemplary display screens might employ specific user interface elements appropriate for the type of information to be conveyed/received by computer system in accordance with the described embodiments, it should be appreciated that the choice of user interface elements for a particular purpose is typically implementation-dependent and/or discretionary. Hence, the illustrated user interface elements employed by any display screens described herein should be considered exemplary in nature, and the reader should appreciate that other user interface elements could be substituted within the scope of various embodiments.

As noted above, in an aspect of certain embodiments, the user interface provides interaction between a user and a computer system. Hence, when this document describes procedures for displaying (or otherwise providing) information to a user, or to receiving input from a user, the user interface may be the vehicle for the exchange of such input/output. Merely by way of example, in a set of embodiments, the user interface allows the user to log on to a master account, access video calling devices via the control server, access videomail and videomail settings/preferences, etc.

In an aspect of some embodiments, the user logs onto his or her master account at the control server in order to access and/or control video calling devices assigned to that account. Accordingly, at block **320**, the method **300** can include authenticating the user with a set of credentials associated with the master account (e.g., with any of several known authentication schemes, such as a userid/password challenge, a certificate exchange process, and/or the like, as well as authentication techniques, described in further detail below, that employ sensors on a video calling device, such as facial recognition, voiceprint analysis, gesture-based identification, spoken identifiers, and/or the like). Once the user has been authenticated, the user interface can present the user with a variety of different information, including without limitation information about status of video calling devices assigned to the master account to which the user has logged on, options for controlling such video calling devices, options for accessing videomail addressed to the user, options for modifying videomail preferences, and/or the like.

Thus, in some aspects, the method **300** might further comprise receiving (e.g., via a network, such as the Internet, to name one example) user preferences (block **325**), and in particular user preferences relating to the access and control of video calling device(s), user preferences for capturing, processing, distributing, or otherwise handling videomail, user preferences for notifying the user regarding videomail, user preferences such as those described above, and/or the like.

29

In some aspects, the method **300** might further comprise receiving (e.g., via a network, such as the Internet, to name one example), a request from the user to (remotely) access a video calling device(s) (block **330**). In an aspect, the user can request such (remote) access by logging into his or her master account and requesting such access through the user interface. The user interface can provide many different mechanisms to allow the user to request access to a video calling device(s). Merely by way of example, the user interface might provide a button or other widget associated with each video calling device assigned to the account, and the user can select the button/widget associated with the video calling device(s) the user would like control. The user interface then can provide options for different types of control that the user can impose on video calling device(s). For instance, the user interface might have a list of commands from which the user can choose text input fields and/or other widgets to select parameters (such as image resolution, number of images to capture, link the video to capture, time and/or interval at which to capture images/video, and/or the like). Based on these examples, the skilled reader can appreciate that the user interface can provide any number of options to allow the user to control the selected video calling device(s).

If the user has assigned multiple video calling devices to the master account, the user might be presented with a list of the assigned devices in the user interface, and receiving the user's request for access to one or more video calling devices can include receiving a selection in the user interface of the one or more video calling devices that the user would like to access. In accordance with some embodiments, the user can access and/or control multiple video calling devices at once (as long as those devices are assigned to the same master account). For example, in an office setting, an administrator might wish to configure multiple video calling devices in the same way (e.g., to enable access by multiple professionals to videomail messages left by clients of the company, and/or the like), and the user interface can allow the administrator to select all desired video calling devices and control all of the selected cameras in the same way or in different ways. In the same manner, the user interface can enable the administrator to establish private and/or secure settings for each professional's video calling device, to establish/modify videomail settings for each individual professional, and/or the like. This functionality can also be used, for example, to update settings in multiple video calling devices at the same time, to update firmware and/or software in multiple video calling devices at the same time, and/or the like.

In a set of embodiments, the method **300** can include accessing the selected video calling device(s) from the control server, over the network (block **335**). Accessing a video calling device(s) can comprise any operation that establishes communication between the control server and the video calling device(s). For instance, as noted above, a video calling device(s) often will be identifiable and/or addressable by an identifier, such as an IP address, etc., and accessing the device can comprise communicating with the video calling device(s) (using any suitable protocol) at the appropriate IP address. In some cases, the control server will establish a secure connection with the video calling device(s). Merely by way of example, in one embodiment, the control server will authenticate the video calling device(s), and/or the video calling device(s) will authenticate the control server (e.g., using a mutual authentication protocol, such as certificate exchange, and/or the like), and/or the control server will establish an encrypted communication session with the video calling device(s) (e.g., using any of a variety of known security

30

techniques, such as secure sockets layer communications, IPSec tunnels, and/or the like).

As noted above, in a set of embodiments, the system can include a software client that can be installed on a computing device that comprises (or is in communication with) a video calling device(s). Examples of such video calling device(s) can include, without limitation, an onboard camera on a tablet, wireless phone, laptop, etc., and/or a separate USB camera, such as a webcam, to provide a couple of examples. Any number of devices that have a software-controllable camera and supports software installation can serve as such a computing device in accordance with different embodiments. In such embodiments, accessing a video calling device(s) can comprise the control server communicating with that software client, which, in turn, can provide the control server with indirect access to the video calling device(s) (e.g., by interfacing with the computing device's operating system framework for controlling the video calling device(s)).

The method **300** can also include controlling the video calling device(s) over the network, based on the user input received via the user interface. Although the method **300** describes the control operations from the perspective of the control server, it should be appreciated that certain embodiments feature video calling devices that operate in response to control by the control server. So, for example, when this document refers to causing a video calling device to take some action, the skilled reader will appreciate that certain embodiments include video calling devices that perform the described action in response to the control input from the control server.

Controlling the video calling device can comprise a variety of operations, and those operations often will depend on what the user has requested. Merely by way of example, in some cases, controlling the video calling device can comprise receiving user input for remotely configuring the video calling device(s) (block **340**). The control server might configure a behavior of the video calling device(s), based on the received user input (block **345**). Such functionality can include causing the video calling device(s) to capture images or video, as described above, but can also include changing an operating parameter of the video calling device(s), such as an address (e.g., IP address) or other identifier of the device, changing or assigning a nickname of the device, changing or assigning an avatar image associated with the device, and/or the like.

In some cases, the control server controls the video calling device(s) by sending one or more command codes to the video calling device(s). These command codes can be used to provide the control described above (such as configuring the video calling device(s), causing the video calling device(s) to determine whether or not the user is available to answer a video call, causing the video calling device(s) to prompt a caller to leave a video mail message, causing the video calling device(s) to record a videomail message from the video call, causing the video calling device(s) to upload the videomail message to a server for post-processing, causing the video calling device(s) to notify the user that he or she has received a videomail message, and/or the like), as well as to provide other commands, such as causing the video calling device(s) to perform a network test and/or perform other suitable operations, such as those described above, as well as operations like checking WiFi signal strength, adjusting camera orientation (e.g., pan, tilt) and/or capture (e.g., focal length, white balance) parameters, changing device configuration (e.g., time zone) parameters, restarting the device, and/or the like. In an aspect, the control server and the video calling device(s) might share a set of command codes, which both devices

31

understand to represent desired commands, and the method **300** can include modifying the set of command codes and/or transmitting the modified set of codes to the video calling device(s). This capability can provide for upgradability and/or advanced remote functionality as new features are developed. Similarly, the control server can transmit updated firmware/software to the video calling device(s) and/or control the video calling device(s) to update its firmware as necessary.

Merely by way of example, in some cases, method **300** might further comprise receiving a request to change user preferences for videomail (block **350**). In response to receiving such a request, method **300** might comprise displaying options related to user preferences for videomail (block **355**), including, without limitation, user preferences for capturing, processing, distributing, or otherwise handling videomail, user preferences for notifying the user regarding videomail, and/or the like. At block **360**, method **300** might comprise receiving user input associated with options related to the user preferences for videomail (displayed at block **355**). Method **300**, at block **365**, might comprise changing the user preferences for videomail, based on the received user inputs (at block **360**).

In some embodiments, method **300** might further comprise receiving a request (from the user) to remotely access videomail (block **370**). In response to such a request, method **300** might, at block **375**, comprise providing the user with remote access to the videomail. In some instances, remote access might include a secure link to a URL addressing the videomail, while in other instances, remote access might include sending a videomail message attached to or embedded in an e-mail notification to the user. In some aspects, at block **380**, method **300** might comprise receiving a request from the user to remotely respond to a videomail message to which the user was provided access at block **375**. At block **385**, method **300** might comprise enabling remote responses to the videomail message, by initiating a video call request to the original caller who left the videomail message, by leaving a videomail message for the original caller (e.g., in the case that the original caller is presently unavailable to answer the video call), by initiating a voice or telephone call to the original caller, by sending an e-mail message to the original caller, by sending a text message to the original caller, and/or the like. Although the embodiments above refer to notification comprising e-mail, the notification can also comprise other forms of communication, including, but not limited to, text messages that include the secure link to the URL addressing the videomail. Herein, text messages might include, without limitation, SMS, MMS, and/or the like.

FIG. 4 illustrates a method **400** of collecting and using presence information, in accordance with one set of embodiments. While the techniques and procedures are depicted and/or described in a certain order for purposes of illustration, it should be appreciated that certain procedures may be reordered and/or omitted within the scope of various embodiments. Moreover, while the method illustrated by FIG. 4 can be implemented by (and, in some cases, are described below with respect to) the system **100** of FIG. 1 (or components thereof), such methods may also be implemented using any suitable hardware implementation. Similarly, while the system **100** of FIG. 1 (and/or components thereof) can operate according to the method illustrated by FIG. 4 (e.g., by executing instructions embodied on a computer readable medium), the system **100** can also operate according to other modes of operation and/or perform other suitable procedures.

Turning to FIG. 4, the method **400** might comprise registering a master account for a user (block **405**). This master

32

account may be the same master account as the master account described in block **305**, or may be a different master account. In accordance with various embodiments, registering a master account for a user can comprise a variety of operations. Merely by way of example, registering a master account can comprise creating a database entry for a particular user and/or assigning authentication credentials to that user; these credentials can be used to access the master account, as described in further detail below.

The method **400** can also include assigning one or more PDDs ("PDDs") to the master account (block **410**). As discussed above, the one or more PDDs can be embodied by a video calling device, such as any of the video calling devices described herein, the VCDs described in the '182 patent, a laptop computer, a desktop computer, a mobile phone, a smart phone, a tablet computer, a video game console, and/or a streaming media player, to name a few non-limiting examples. For instance, the user might identify any PDDs that the user owns (or is otherwise associated with; e.g., members of the user's family might be associated with the devices owned by the user), and the system can assign those PDDs to the user's master account. According to some embodiments, the user's master account might include any suitable number of sub-accounts. In one example, each member of the user's family might be associated with a sub-account linked with the master account. In some instances, the user (or some members of his or her family) might have a work/school sub-account and a home sub-account, the former being associated with profiles and/or media content appropriate for school or work, while the latter being associated with all, or all other, profiles and/or media content. In some embodiments, the master account and the plurality of sub-accounts might be organized as a hierarchy, with the master account (being at the top of the hierarchical structure) having full access to profiles and media content of each sub-account, the sub-accounts at the next level having access to profiles and/or media content of only those sub-accounts that the master account has given access to, and the sub-accounts at lower levels having limited access to profiles and/or media content. For example, the user's master account might have access to all profiles and/or media content associated with the master account and the sub-accounts. The user can provide his or her spouse with a sub-account having the same access to profiles and/or media content, while providing limited access to profiles and/or media content to each of the user's children's sub-account(s). In some instances, the user and/or the user's spouse might impose limits on access to profiles and/or media content for each of their work sub-accounts.

In some cases, each PDD might have an identifier, such as a hardware identifier, IP address, nickname, and/or the like, by which the system can address the PDD, and assigning a PDD to the master account can comprise associating that identifier with the master account. When a PDD is assigned to a master account, the user of that account will be able to access, configure, and/or control the PDD through the control server, for example as described in further detail below. In some cases, the user might own a plurality of PDDs and might wish to control all of the PDDs from a single master account. In an aspect, a user can identify such devices through a user interface to the control server.

In another aspect, as described briefly above, the assignment process can be simplified. When the user first configures a PDD (usually locally, but perhaps over the network), the user can provide credentials to the PDD that associate the device with the master account. Thereafter, the PDD might be configured to communicate with the control server and identify itself using those credentials; at that point, the control

server can assign the PDD to the master account, and no credentials need to be stored on the PDD from that point forward (other than perhaps the PDD's own identifying information).

Hence, the method **400**, in the illustrated embodiment, might further comprise providing a user interface to allow interaction between the user and the control server (block **415**). For example, the user interface can be used to output information for a user, e.g., by displaying the information on a display device, printing information with a printer, playing audio through a speaker, etc.; the user interface can also function to receive input from a user, e.g., using standard input devices such as mice and other pointing devices, motion capture devices, touchpads and/or touchscreens, keyboards (e.g., numeric and/or alphabetic), microphones, etc. The procedures undertaken to provide a user interface, therefore, can vary depending on the nature of the implementation; in some cases, providing a user interface can comprise displaying the user interface on a display device; in other cases, however, in which the user interface is displayed on a device remote from the computer system (such as on a client computer, wireless device, etc.), providing the user interface might comprise formatting data for transmission to such a device and/or transmitting, receiving, and/or interpreting data that is used to create the user interface on the remote device. Alternatively and/or additionally, the user interface on a client computer (or any other appropriate user device) might be a web interface, in which the user interface is provided through one or more web pages that are served from a computer system (and/or a web server in communication with the computer system), and are received and displayed by a web browser on the client computer (or other capable user device). The web pages can display output from the computer system and receive input from the user (e.g., by using Web-based forms, via hyperlinks, electronic buttons, etc.). A variety of techniques can be used to create these Web pages and/or display/receive information, such as JavaScript, Java applications or applets, dynamic Hypertext Markup Language ("HTML") and/or Asynchronous JavaScript and XML (or extensible markup language) ("AJAX") technologies, to name but a few examples.

In many cases, providing a user interface will comprise providing one or more display screens each of which includes one or more user interface elements. As used herein, the term "user interface element" (also described as a "user interface mechanism" or a "user interface device") means any text, image, or device that can be displayed on a display screen for providing information to a user and/or for receiving user input. Some such elements are commonly referred to as "widgets," and can include, without limitation, text, text boxes, text fields, tables and/or grids, menus, toolbars, charts, hyperlinks, buttons, lists, combo boxes, checkboxes, radio buttons, and/or the like. While any illustrated exemplary display screens might employ specific user interface elements appropriate for the type of information to be conveyed/received by computer system in accordance with the described embodiments, it should be appreciated that the choice of user interface elements for a particular purpose is typically implementation-dependent and/or discretionary. Hence, the illustrated user interface elements employed by any display screens described herein should be considered exemplary in nature, and the reader should appreciate that other user interface elements could be substituted within the scope of various embodiments.

As noted above, in an aspect of certain embodiments, the user interface provides interaction between a user and a computer system. Hence, when this document describes proce-

dures for displaying (or otherwise providing) information to a user, or to receiving input from a user, the user interface may be the vehicle for the exchange of such input/output. Merely by way of example, in a set of embodiments, the user interface allows the user to log on to a master account, access PDDs via the control server, access videomail and videomail settings/preferences, etc.

In an aspect of some embodiments, the user logs onto his or her master account at the control server in order to access and/or control PDDs assigned to that account, and/or access videomail and videomail preferences. Accordingly, at block **420**, the method **400** can include authenticating the user with a set of credentials associated with the master account (e.g., with any of several known authentication schemes, such as a userid/password challenge, a certificate exchange process, and/or the like, as well as authentication techniques, described in further detail below, that employ sensors on a PDD, such as facial recognition, voiceprint analysis, gesture-based identification, spoken identifiers, and/or the like). Once the user has been authenticated, the user interface can present the user with a variety of different information, including without limitation information about status of PDDs assigned to the master account to which the user has logged on, options for controlling such PDDs, options for accessing videomail addressed to the user, options for modifying videomail preferences, and/or the like.

Thus, in some aspects, the method **400** might further comprise receiving (e.g., via a network, such as the Internet, to name one example) user preferences (block **425**), and in particular user preferences relating to the collection and/or use of presence information, including without limitation preferences such as those described above. The method **400**, then, can further include controlling and/or configuring the PDD, in some cases based at least in part on the user preferences (block **430**). In some embodiments, the user preferences might include user preferences for capturing, processing, distributing, or otherwise handling videomail, user preferences for notifying the user regarding videomail, and/or the like. Merely by way of example, the user might have specified in the user preferences that the PDD should not be used to collect presence information at all, in which case that feature might be turned off at the PDD. In the case that the user preferences indicate that presence information should be turned off (e.g., privacy settings may be set high, either permanently or temporarily, and/or with respect to certain user-established and/or preset conditions, or the like), some embodiments might establish a blocking feature for the user when other PDDs send presence information for comparison matching processes with database user biometrics, the effect of which being that no match can be made, and thus the user's profiles and/or media content (and/or access thereto) is not ported to the other PDDs. Alternatively and/or additionally, the user might have specified some limitations on the collection of presence information (such as about whom such information may be collected, times at which information can be collected, and/or purposes for which information may be collected, to name a few examples). Of course, in some embodiments, these preferences can be set directly at the PDD, e.g., through a menu system displayed on a video device. It should also be recognized that some preferences (such as with whom presence information can be shared) might not affect the PDD and might be saved and/or operated on at the control server instead.

The amount of control imposed by the control server can vary according to embodiment and implementation. Merely by way of example, as noted above, in some embodiments, there might be no control server, and the PDD might incor-

porate all the functionality described herein with regard to the control server, including peer-to-peer functionality with other PDDs. In other embodiments, the control server might provide fairly fine-grained control over the PDD, such as instructing the camera to capture images for purposes of determining presence, and/or the control server may receive the images directly and perform the presence determination, identification, and/or authentication procedures at the control server. The division of responsibility between the control server and the PDD can fall anywhere along this spectrum. In some cases, for instance, the control server might provide the user preferences to the PDD, which then is responsible for collecting presence information in accordance with those preferences and transmitting the presence information to the control server, which takes the appropriate action in response to the presence information, such as selecting an advertisement based on the presence information. Alternatively and/or additionally, the PDD itself might be responsible for taking such actions.

At block 435, the method 400 can comprise collecting presence information. A variety of operations might be involved in the collection of presence information. For example, in some cases, the PDD captures one or more images of at least a portion of a room where it is located and/or of a user present in the room (block 440). Such images can be digital still images, a digital video stream, and/or the like. In other cases, the method can include capturing audio samples (block 445), identifying devices in proximity to the capturing device (block 450), and/or the like (for example as described above).

The method 400 can further comprise analyzing one or more of the collected presence information (block 455), including one or more of the images, video samples, audio samples, etc. Merely by way of example, the images and/or video samples might be analyzed with facial recognition software and/or other biometric/physiological recognition software, which can be used to determine the number of people in the room with the PDD and/or to identify any of such people (e.g., by determining a name, an age range, a gender, and/or other identifying or demographic information about a user, based on the output of the facial recognition software and/or other biometric/physiological recognition software). Alternatively and/or additionally, analyzing the images can comprise determining that a person is watching a display device, for example using eye-tracking software to identify a focus area of the person's eyes and correlating that focus area with the location on a screen or display of a television (or other suitable display device). In some cases, if the number of people and the identities (or at least demographic characteristics) of each of the people in the room can be determined, analyzing the images can further include determining a collective demographic of the people in the room (based, for example, on the demographic characteristics of a majority of people in the room). In further cases, the method might analyze audio samples using voiceprint analysis, compare user responses to stored challenge/response information, and/or the like. As yet another example, a camera of a PDD might capture user gestures, which can be compared with stored gestures (e.g., a particular pattern of hand waving, a pattern of fingers displayed by the user, etc.) in a gesture-based identification and/or authentication scheme. It should be noted that many embodiments can use various combinations of such techniques (such as a combination of facial analysis and spoken, gestured, or typed identifiers, to name a few examples) to provide two-factor authentication.

Such analysis can be performed at the PDD and/or at the control server. Accordingly, in some embodiments, the PDD

will transmit presence information or other identifying information that can be used (in part or in whole) for identifying the user. Such identifying information can include raw or analyzed presence information, as well as information derived from the presence information, such as, to name some examples, extracted features from an image, audio segment, and/or video segment; an excerpted image, video, and/or audio segment; and/or the like. Such presence information and/or identifying information can be transmitted from the PDD to the control server (block 460), although as noted above, this is not necessary in some embodiments (e.g., where identifying the user or other analysis is performed at the PDD). Such transmission might comprise IP communications over the Internet, (perhaps over a secure channel, such as a virtual private network ("VPN")), and, as noted above, the presence/identifying information can include a wide variety of different types of information that enable the control server to determine presence and/or identify/authenticate a user. Hence, at block 465, the control server (in a cloud-based presence detection scheme) might receive the transmitted presence information. In the case that raw presence information is received by the control server, the control server might analyze the raw presence information in a similar manner as described above at block 455. At block 470, the method 400 comprises detecting and/or determining presence of a user. This determination can be made by the PDD and/or by the control server. In one case, for example, the PDD might transmit raw video segments, raw images, raw audio samples, etc. to the server, which might perform all analysis and presence determination. In another case, the PDD might perform this analysis and might notify the control server that a user is present. Receiving such a notification at the control server can be considered to be the control server detecting presence of a user.

At block 475, the method 400 can include identifying and/or authenticating a user. In some cases, this identification and/or authentication can be implicit in the operation of detecting user presence. For example, in performing facial recognition to detect that a user is present, the PDD (and/or control server) might further analyze the same image to determine an identity of the present user. Alternatively, however, detection of user presence and identification/authentication of the user might be performed as discrete steps (and might depend on device capabilities). For example, a PDD might have sufficient capabilities to detect the presence of the user, and if so, might send identifying information (such as a captured image, video sample, audio sample, etc.) to the control server to actually identify the user. Alternatively, the PDD might be capable of identifying the user on its own and might merely send the identity of the user (i.e., data identifying the user, such as a name, username, etc.) to the server.

In some instances, the PDD and/or the control server (i.e., in a cloud-based presence scheme) might have access to the user's profile or other personal information of the user (including, without limitation, communications, calendar items, contacts list, travel/itinerary information, IP address of user's PDD(s), or the like). Such profile or other personal information might indicate that the user is visiting a friend or relative in a different city, state, or country. In the case that the friend or family member has a similar PDD linked to a common network with the control server or other PDDs (i.e., in a peer-to-peer or distributed computing scheme), the user's PDD and/or the control server (if present) might facilitate identification and/or authentication of the user at the friend's or relative's PDD ("other PDD"), by, for example, sending the user's biometric/physiological information to the other PDD and/or to a data center local to the other PDD, so as to

reduce comparison/matching times for identification/authentication of the user at the other PDD. Such proactive autonomous facilitation functionality might, in some cases, be subject to the user's selection of such option in the user preferences (e.g., at block 425 above). In some cases, the user might disable and/or limit such functionality (e.g., for privacy reasons, for security reasons, and/or the like). In some embodiments, the IP address of a PDD at which a user attempts to log in might be analyzed to determine the city in which the PDD is located. If the city (or neighborhood or customer premises) of the last PDD at which the user logged in (or is otherwise authenticated by) is determined to be different from the city (or neighborhood or customer premises) of the current PDD, then it can be inferred that the user has moved, or is travelling. Such inference may be used, in some embodiments, to further infer a general direction in which the user is travelling (or to infer a potential destination(s), if sufficient numbers of data points/locations are determined), and can be used to send ahead the user's profile and/or content to control servers and/or PDDs that are at or near the determined potential destination(s).

Once the present user has been identified and/or authenticated, the control server (and/or the PDD at which the user is present) might enabling or implementing video mail capture, processing, and distribution over the network, in accordance with any or all of the processes in blocks 305-385, as described in detail above with respect to FIG. 3.

Alternatively, in some embodiments, the PDD and the video calling device might be the same user device, in which case, the video calling device might detect presence of a user (as described in detail above with respect to the PDD), and might notify a computer about the detected presence of a user. Such a video calling device might then receive, over a network, control instructions from the computer to enable or implement video mail capture, processing, and distribution, based on the detected presence of the user.

According to some aspects, in response to determining the presence of the user (at block 470) and/or identifying and authenticating the user (at block 475), method 400 might further comprise enabling remote access to the video calling device and/or remote access to user preferences over the network (block 480). In some cases, the user preferences might include preferences related to videomail and/or videomail settings. At block 485, method 400 might comprise enabling remote access to videomail over the network, in some cases, in response to determining the presence of the user (at block 470) and/or identifying and authenticating the user (at block 475).

In some embodiments, the method 400 might further comprise determining that a user is no longer present at the PDD (block 490). For example, as noted above, the system might continuously and/or periodically capture images and perform presence determination techniques (e.g., as described above) to determine whether the user is still present, and/or might actively query the user after some period of time to determine whether the user is still present. If the system determines that the user is no longer present, the system can block remote access (and control) of the video calling device(s) from the PDD, remote access to user preferences, and remote access to videomail, over the network (block 495). For example, the system might delete any image or video content transmitted from the video calling device(s) to the device, log out of any services for controlling the video calling device(s) that the system had logged into from the PDD, revoke access to image and/or video content captured by the video calling device(s) (and/or post-processed using raw captured image data or raw captured video data from the video calling device(s)) stored in

the cloud, revoke access to view or modify user preferences (including user preferences related to videomail), revoke access to view or respond to videomail, and/or the like. This functionality is particularly useful and applicable to PDDs (or other devices) that are neither owned nor associated with the user (e.g., a friend's or relative's device, devices at a vacation hotel or vacation rental property, etc.). Such determination and content/access removal might, in some instances, be based on a time-out system (e.g., 5, 15, 30, or 80 minutes, etc.), in which the system might account for the user's temporary absence from the room, while protecting the access to profiles (with which accessing and control of the video calling device(s) may be associated and/or with which videomail and videomail preferences may be associated), videomail messages, and/or content. In some cases, the user can select specific time-out periods, which can be stored in the user's profile, and such specific time-out periods can be universally applicable to some or all profiles, some or all media content, or some or all profiles and media content, some or all videomail messages, some or all preferences related to videomail, or can be specific to particular profiles and/or media content. In some cases, user profiles might be associated with a much shorter time-out period (a time between 1-5 minutes) compared with media content (which might have a time-out period ranging from 15 minutes to 3 hours, or the like). The time-out system might be based on a counter or clock system that starts counting from the last time the system recognized that the user was in range of any of the sensors of the PDD. Any suitable techniques other than the time-out system described above may be implemented as appropriate.

The reader should note that a wide variety of presence-based functions (including without limitation those described in the Related Applications) can be performed by the system in conjunction with various techniques described as part of the methods 200, 300, and/or 400, and that such functions can be combined in any suitable way. Merely by way of example, the '603 application described advertising techniques that can be implemented based on detected presence, and such techniques can be integrated with various techniques described as part of the method 200, method 300, and/or method 400. For instance, the system (e.g., the control server, the PDD, the video calling device, etc.) might obtain relevant advertising material as described in the '603 application and display such advertising over content obtained and delivered using the techniques of the method 200, method 300, and/or method 400. Based on this disclosure, the skilled reader will understand that such techniques can be combined in a number of different ways.

FIG. 5 illustrates a functional diagram of a system 500 for enabling or implementing video mail capture, processing, and distribution, in accordance with various embodiments. The skilled reader should note that the arrangement of the components illustrated in FIG. 5 is functional in nature, and that various embodiments can employ a variety of different structural architectures. Merely by way of example, one exemplary, generalized architecture for the system 500 is described below with respect to FIG. 8, but any number of suitable hardware arrangements can be employed in accordance with different embodiments.

In FIG. 5, a video calling device 505 might correspond to video calling device 105 and/or PDD 105, while user device 545 might correspond to non-video calling device or non-PDD user device 105, as described in detail above with respect to FIG. 1. Control server 510, network 515, and cloud storage system 530, in the example of FIG. 5, might corre-

spond to control server **110**, network **115**, and cloud storage system **130**, respectively, as described in detail above with respect to FIG. **1**.

System **500** might further comprise a local content source **535** (e.g., a local content source as described above), a display device **540** (including, without limitation, a television (“TV”) and/or the like), and high-definition (“HD”) data cables **550** (or any other suitable data transmission media). In some cases, the HD data cables **550** might include, without limitation, high-definition multimedia interface (“HDMI”) cables. One or more of the video calling devices **505** (e.g., the first video calling device **505a** and the third video calling device **505c**, as shown in FIG. **5**) might be configured to provide pass-through audio and/or video from a local content source **535** to a display device **540** (e.g., using data cables **550**). Merely by way of example, in some embodiments, an HDMI input port in the video calling device **505** allows HD signals to be input from the corresponding local content source **535**, and an HDMI output port in the video calling device **505** allows HD signals to be output from the video calling device **505** to the corresponding display device **540** (e.g., TV, which might include, but is not limited to, an Internet Protocol TV (“IPTV”), an HDTV, a cable TV, or the like). The output HD signal may, in some cases, be the input HD signal modified by the video calling device **505**. Local content source **535** might be any suitable local content source. As noted above, a local content source can be any device that provides an audio or video stream to a display device and thus can include, without limitation, a cable or satellite STB, an IPTV STB, devices that generate video and/or audio, and/or acquire video and/or audio from other sources, such as the Internet, and provide that video/audio to a display device; hence a local content source can include devices such as a video game console, a Roku® streaming media player, an AppleTV®, and/or the like. Hence, when situated functionally inline between a local content source and a display device, the video calling device **505** can receive an audiovisual stream output from the local content source, modify that audiovisual stream in accordance with the methods described in the ’182 patent, and provide the (perhaps modified) audiovisual stream as input to the display device **540**. In some embodiments, first video calling device **505a**, local content source **535a**, display device **540a**, and user device **545a** (if any) might be located at a first customer premises **560a**, while third video calling device **505c**, local content source **535c**, display device **540c**, and user device **545c** (if any) might be located at a third customer premises **560c**. According to some embodiments, the second video calling device **505b**, which in the context of the various embodiments refers to the calling device associated with the caller, might be located at a second customer premises **560b**. In some instances, the second video calling device **505b** might be a portable user device (including, without limitation, a tablet computer, a laptop computer, a smart phone, a mobile phone, a portable gaming device, and/or the like) that is not bound to any particular customer premises **560**.

According to some embodiments, system **500** might further comprise one or more access points (not shown), each of which might be located in proximity to or in the first customer premises **560a**, the second customer premises **560b**, and/or the third customer premises **560c**. The access point(s) can allow wireless communication between each video calling device **505** and network **515**. (Of course, a video calling device **505** might also have a wired connection to an access point, router, residential gateway, etc., such as via an Ethernet cable, which can provide similar communication functionality.) In some cases (as shown), each video calling device **505** might be communicatively coupled to network **515** (via either

wired or wireless connection), without routing through any access points. In some cases, wired or wireless access to network **515** allows video calling device **505** to obtain profiles from cloud storage system **530** and/or media content from content server **570** and media content database **575** independent of the corresponding local content source **535**, which is in communication with a television (“TV”) distribution network **565** (either via wireless connection or via wired connection). In some cases (not shown), TV distribution network **565** (which could be, for example, a cable television distribution network, a satellite television distribution network, an Internet Protocol television (“IPTV”) distribution network, and/or the like) might be communicatively coupled with content server **570**, and thus local content source **535** might obtain media content from content server **570** and media content database **575** independently of video calling device **505**. Alternatively or in addition, the television distribution network **565** might be communicatively coupled to other content servers and/or other media content sources (not shown).

In this manner, video calling device **505** can overlay the input signal from the corresponding local content source **535** with additional media content to produce an augmented output HD signal to the corresponding display device **540** via data cables **550**. This functionality allows for supplemental content (which may be associated with the media content accessed by the local content source **535** for display on display device **540**) to be accessed and presented using the first video calling device **505**, in some cases, as a combined presentation on the display device **540**, which may be one of an overlay arrangement (e.g., a picture-in-picture (“PIP”) display, with the supplemental content overlaid on the main content), a split screen arrangement (with the supplemental content adjacent to, but not obscuring any portion of the main content), a passive banner stream (with non-interactive supplemental content streaming in a banner(s) along one or more of a top, bottom, left, or right edge of a display field in which the main content is displayed on display device **540**), and/or an interactive banner stream (with interactive supplemental content streaming in a banner(s) along one or more of a top, bottom, left, or right edge of a display field in which the main content is displayed on display device **540**). Herein, examples of interactive supplemental content might include, without limitation, content that when streamed in a banner can be caused to slow, stop, and/or replay within the banner, in response to user interaction with the content and/or the banner (as opposed to passive banner streaming, in which information is streamed in a manner uncontrollable by the user). The interactive supplemental content that is streamed in the banner may, in some instances, also allow the user to invoke operations or functions by interacting therewith; for example, by the user highlighting and/or selecting the supplemental content (e.g., an icon or still photograph of a character, actor/actress, scene, etc. associated with the main content), links for related webpages, links to further content stored in media content database **575**, or operations to display related content on display device **540** and/or user device **545** may be invoked.

In some instances, video calling device **505** might detect the presence and/or proximity of one or more user devices **545** associated with the user, and might (based on user profile information associated with the user that is stored, e.g., in cloud storage system **530**) automatically send supplemental media content via wireless link **555** (directly from video calling device **505** or indirectly via an access point (not shown)) for display on a display screen(s) of the one or more user devices **545**. In one non-limiting example, a user asso-

ciated with first video calling device **505a** might have established a user profile stored in cloud storage system **530** that indicates a user preference for any and all supplemental content for movies and television programs to be compiled and displayed on one or more user devices **545a** (including, but not limited to, a tablet computer, a smart phone, a laptop computer, and/or a desktop computer, etc.) concurrent to display of the movie or television program being displayed on display device **540a**. In such a case, when a movie is playing on display device **540a** broadcast or streamed via local content source **535a** from content server **570** and media content database **575** (and/or from some other content server and some other media content source) via network **565**, first video calling device **505a** accesses supplemental content (if available) from content server **570** and media content database **575** via network **515**, and sends the supplemental content to the user's tablet computer and/or smart phone via wireless link(s) **555**. For example, bios of actors, actresses, and/or crew might be sent to the user's smart phone for display on the screen thereof, while schematics of machines, weapons, robots, tools, etc. associated with the movie or television show might be sent to and displayed on the user's tablet computer, behind the scenes videos or information, news/reviews associated with the main content, and/or music videos associated with the main content may also be sent to the user's smart phone and/or tablet computer, and so on.

In some embodiments, the first video calling device **505a** (which, in the context of the embodiments herein, is associated with a user or callee) and the second video calling device **505b** (which, in the context of the embodiments herein, is associated with a caller) might be of different make and/or model (i.e., might be made by different manufacturers, might be of different models by the same manufacturer, and/or the like). According to some aspects, the second video calling devices **505b** might have functionality similar to video calling device **105** and/or PDD **105**, but may or may not necessarily possess pass-through capability between a display device and a local content source, as described above with respect to the first and third video calling devices **505a** and **505c**.

According to some embodiments, the detection of the presence of the user device **545** by the first video calling device **505a** and/or the third video calling device **505c** might allow identification of a user and thus access of profiles, content, and/or videomail associated with the user's account, regardless of whether the first video calling device **505a** or the third video calling device **505c** is owned by and/or associated with the user. Herein, the user's media content might include, without limitation, at least one of purchased video content, purchased audio content, purchased video game, purchased image content, rented video content, rented audio content, rented video game, rented image content, user-generated video content, user-generated audio content, user-generated video game content, user generated image content, and/or free media content, while the user's profiles might include, but is not limited to, one or more of user profile information for a video game or video game console, web browser history and/or bookmarks, contact information for the user's contacts, user profile information for video or audio content, including without limitation recommended content, device preferences, videomail preferences, user profile information for cloud services, and/or the like. Videomail, herein, might refer to videomail messages addressed to the user or callee. In some cases, the user's profile might also include identifying information—including, but not limited to, the user's biometric information (e.g., facial characteristics, voice characteristics, fingerprint characteristics, iris characteristics, pupil characteristics, retinal characteristics, etc.), or the like. In

some examples, the user profile information for cloud services might include user log-in information (e.g., username, account number, and/or password/passphrase, etc.) or other suitable credentials for cloud services, which might include, without limitation, video calling service, videomail service, voice calling service, video broadcast/streaming service, audio broadcast/streaming service, on-line gaming service, banking/financial services, travel/accommodation/rental vehicle services, and/or dining/entertainment event reservation/ticketing services, or the like.

In one example, a user might be associated with first video calling device **505a** (located in the first customer premises **560a**), while her friend might be associated with third video calling device **505c** (located in the third customer premises **560c**), and the user and the friend are both subscribers of a similar service provided by control server **510** and/or the cloud service provider associated with control server **510**. When the user visits her friend, the friend's video calling device **505c** might first detect presence of the user, by querying and/or obtaining the identification information for the user's smart phone and/or tablet computer or the like, by capturing video, image, and/or voice data of the user, by infrared detection of a living person in the room, and/or by audio detection of a living person in the room, etc. The friend's video calling device **505c** might then identify the user using the user's device(s) identification information and/or the captured video, image, and/or voice data, or might send such presence information to control server **510** for identification and authentication analysis. In some cases, detecting presence of, or identifying/authenticating, the user might include, without limitation, analyzing captured images or video segments using one or more of facial recognition software, pupil/iris recognition software, retinal identification software, fingerprint analysis software, and/or physiology recognition software, analyzing captured audio samples using one or more of voiceprint analysis and/or comparison with stored challenge/response information, and/or identification of a user device owned by and/or associated with the user (e.g., based on identification information of the device, which may be previously associated with the user or the user's profile(s), etc.). In terms of detection of the presence of the user's device, any suitable technique may be implemented including, but not limited to, at least one of detecting a Bluetooth connection of the user device, detecting that the user device is associated with a WiFi access point with which the video calling device has associated, and/or communicating with the user device using near field communication ("NFC").

Once the user has been identified and authenticated, control server **510** might send copies of the user's profiles and/or content to the third video calling device **505c** (either from first video calling device **505a** and/or from cloud storage system **530**, or the like), or at least provide the user with access to her profiles, videomail, and/or content from her friend's video calling device **505c**. In some embodiments, the identification and authentication processes might include comparing the user device identification information and/or the captured video, image, and/or voice data against all similar identification data for all users/subscribers of the cloud service that are stored in cloud storage system **530**. In some cases, the process might be facilitated where video calling devices **505a** and **505c** might already be associated with each other (e.g., where the user has previously made a video call from first video calling device **505a** to her friend on third video calling device **505c**, where the user might have added the friend to the user's contact list, and/or where the friend might have added the user to the friend's contact list). In other cases, the user's first

video calling device **505a** might have access to the user's calendar and/or communications, which might indicate that the user is visiting the friend. The first video calling device **505a** might query control server **510** to determine whether the friend has a video calling device **505c** associated with the cloud service provider. In this example, the first video calling device **505a** determines that third video calling device **505c** is part of the same service and/or is in communication with control server **510**, and based on such determination, first video calling device **505a** (and/or control server **510**) might send the user's profiles and/or content to third video calling device **505c**, and/or provide third video calling device **505c** with access to the user's profiles, videomail, and/or content. In some embodiments, the user's profiles, videomail, and/or content, or access to profiles, videomail, and/or content, might be encrypted, and might be released/decrypted upon identification and/or authentication by third video calling device **505c** (and/or by control server **510**) when the user is detected by third video calling device **505c**. In this manner, the user's profiles, videomail, and/or content can follow the user wherever she goes, so long as there is a device (e.g., video calling device) that is associated with the same or affiliate cloud service provider at her destination, and so long as the device can recognize and authenticate the user.

By the same token, if the user is no longer detected by the third video calling device **505c**, either after a predetermined number of prompts or queries for the user and/or after a predetermined period of time (e.g., after a specified number of minutes, hours, days, weeks, months, etc.), third video calling device **505c** (and/or control server **510**) might determine that the user is no longer present at the location of third video calling device **505c**. Based on such a determination, third video calling device **505c** and/or control server **510** might remove the user's profiles, videomail, and/or media content (or access thereto) from third video calling device **505c**. As described above, a time-out system might be utilized. Alternatively, other suitable systems may be used for determining the user is no longer present, and removing the user's profiles, videomail, and/or media content (or access thereto) from the third video calling device **505c**.

FIGS. **6A** and **6B** (collectively, "FIG. **6**") are illustrations of user devices **600** used by users that present exemplary graphical user interfaces, in accordance with various embodiments. In particular, FIG. **6A** is an illustration of a user device used by users that presents an exemplary graphical user interface for notifying users regarding videomail messages, while FIG. **6B** is an illustration of a user device used by users that present an exemplary graphical user interface for present options related to a user's master account, the user's devices, videomail, and account settings.

In FIG. **6**, although each user device **600** is shown as a smart phone, the various embodiments are not so limited, and user devices **600** might be any suitable user device comprising, without limitation, an HDTV, an IPTV, a cable TV, a desktop computer, a laptop computer, a tablet computer, a mobile phone, a portable gaming device, other suitable user devices, or any combination of these user devices.

User device **600** might comprise device housing **605**, a display screen **605a**, and the like. In some embodiments, display screen **605a** might comprise a touchscreen display, a non-touchscreen display, and/or the like. In the examples of FIG. **6**, a panel **610** of a graphical user interface ("GUI") might present a message or notification from the service provider (in this example, the videomail service provider) to the user indicating that the user or callee associated with the user device **600** (and associated with the first video calling device **505a**) has received a new videomail message(s) from

a caller. The panel **610** or notification might provide the user or callee with links to access the videomail message(s) and/or to access the user's or callee's account information (including, without limitation, master account information, user profiles, user preferences related to videomail, videomail messages, and/or the like). In some cases, the links include one or more universal resource locators ("URLs") addressing the videomail message(s), which in some cases have been post-processed (after recording) to be compatible with most (if not all) formats, play-back devices, resolutions, and/or the like.

In the embodiment illustrated in FIG. **6**, a panel **615** might represent a user's or callee's accounts page, which might include options **620**, which might comprise, but are not limited to, options pertaining to the user's devices, options for accessing videomail, options for modifying account settings (including master account settings, user profile settings, user preferences, videomail preferences, and/or the like), and/or an option to logout of the user's account page, or the like. In some embodiments, the options for accessing videomail might include, but are not limited to, options to view one or more videomail messages, options to mark one or more videomail messages as being viewed, options to mark one or more videomail messages as being not yet viewed, options to respond to one or more videomail messages, options to delete one or more videomail messages, and/or the like. According to some aspects, the videomail preferences might include, without limitation, preferences for notifying the user of any new or not yet viewed videomail messages, preferences related to prompting callers to leave videomail messages, preferences for recording videomail prompts, preferences related to post-processing of videomail messages, and/or the like.

FIG. **7** provides a schematic illustration of one embodiment of a computer system **700** that can perform the methods provided by various other embodiments, as described herein, and/or can function as a video calling device, a PDD, user device, control server, web server, and/or the like. It should be noted that FIG. **7** is meant only to provide a generalized illustration of various components, of which one or more (or none) of each may be utilized as appropriate. FIG. **7**, therefore, broadly illustrates how individual system elements may be implemented in a relatively separated or relatively more integrated manner.

The computer system **700** is shown comprising hardware elements that can be electrically coupled via a bus **705** (or may otherwise be in communication, as appropriate). The hardware elements may include one or more processors **710**, including without limitation one or more general-purpose processors and/or one or more special-purpose processors (such as digital signal processing chips, graphics acceleration processors, and/or the like); one or more input devices **715**, which can include, without limitation, a mouse, a keyboard, and/or the like; and one or more output devices **720**, which can include, without limitation, a display device, a printer, and/or the like.

The computer system **700** may further include (and/or be in communication with) one or more storage devices **725**, which can comprise, without limitation, local and/or network accessible storage, and/or can include, without limitation, a disk drive, a drive array, an optical storage device, solid-state storage device such as a random access memory ("RAM") and/or a read-only memory ("ROM"), which can be programmable, flash-updateable, and/or the like. Such storage devices may be configured to implement any appropriate data stores, including, without limitation, various file systems, database structures, and/or the like.

The computer system **700** might also include a communications subsystem **730**, which can include, without limitation, a modem, a network card (wireless or wired), an infrared communication device, a wireless communication device and/or chipset (such as a Bluetooth™ device, an 802.11 device, a WiFi device, a WiMax device, a WWAN device, cellular communication facilities, etc.), and/or the like. The communications subsystem **730** may permit data to be exchanged with a network (such as the network described below, to name one example), with other computer systems, and/or with any other devices described herein. In many embodiments, the computer system **700** will further comprise a working memory **735**, which can include a RAM or ROM device, as described above.

The computer system **700** also may comprise software elements, shown as being currently located within the working memory **735**, including an operating system **740**, device drivers, executable libraries, and/or other code, such as one or more application programs **745**, which may comprise computer programs provided by various embodiments, and/or may be designed to implement methods, and/or configure systems, provided by other embodiments, as described herein. Merely by way of example, one or more procedures described with respect to the method(s) discussed above might be implemented as code and/or instructions executable by a computer (and/or a processor within a computer); in an aspect, then, such code and/or instructions can be used to configure and/or adapt a general purpose computer (or other device) to perform one or more operations in accordance with the described methods.

A set of these instructions and/or code might be encoded and/or stored on a non-transitory computer readable storage medium, such as the storage device(s) **725** described above. In some cases, the storage medium might be incorporated within a computer system, such as the system **700**. In other embodiments, the storage medium might be separate from a computer system (i.e., a removable medium, such as a compact disc, etc.), and/or provided in an installation package, such that the storage medium can be used to program, configure, and/or adapt a general purpose computer with the instructions/code stored thereon. These instructions might take the form of executable code, which is executable by the computer system **700** and/or might take the form of source and/or installable code, which, upon compilation and/or installation on the computer system **700** (e.g., using any of a variety of generally available compilers, installation programs, compression/decompression utilities, etc.) then takes the form of executable code.

It will be apparent to those skilled in the art that substantial variations may be made in accordance with specific requirements. For example, customized hardware (such as programmable logic controllers, field-programmable gate arrays, application-specific integrated circuits, and/or the like) might also be used, and/or particular elements might be implemented in hardware, software (including portable software, such as applets, etc.), or both. Further, connection to other computing devices such as network input/output devices may be employed.

As mentioned above, in one aspect, some embodiments may employ a computer system (such as the computer system **700**) to perform methods in accordance with various embodiments of the invention. According to a set of embodiments, some or all of the procedures of such methods are performed by the computer system **700** in response to processor **710** executing one or more sequences of one or more instructions (which might be incorporated into the operating system **740** and/or other code, such as an application program **745**) con-

tained in the working memory **735**. Such instructions may be read into the working memory **735** from another computer readable medium, such as one or more of the storage device(s) **725**. Merely by way of example, execution of the sequences of instructions contained in the working memory **735** might cause the processor(s) **710** to perform one or more procedures of the methods described herein.

According to some embodiments, system **700** might further comprise one or more sensors **750**, which might include, without limitation, one or more cameras, one or more IR sensors, and/or one or more 3D sensors, or the like. In some cases, the one or more sensors **750** might be incorporated in (or might otherwise be one of) the input device(s) **715**. The output device(s) **720** might, in some embodiments, further include one or more monitors, one or more TVs, and/or one or more display screens, or the like.

The terms “machine readable medium” and “computer readable medium,” as used herein, refer to any medium that participates in providing data that causes a machine to operate in a specific fashion. In an embodiment implemented using the computer system **700**, various computer readable media might be involved in providing instructions/code to processor(s) **710** for execution and/or might be used to store and/or carry such instructions/code (e.g., as signals). In many implementations, a computer readable medium is a non-transitory, physical, and/or tangible storage medium. Such a medium may take many forms, including, but not limited to, non-volatile media, volatile media, and transmission media. Non-volatile media includes, for example, optical and/or magnetic disks, such as the storage device(s) **725**. Volatile media includes, without limitation, dynamic memory, such as the working memory **735**. Transmission media includes, without limitation, coaxial cables, copper wire and fiber optics, including the wires that comprise the bus **705**, as well as the various components of the communication subsystem **730** (and/or the media by which the communications subsystem **730** provides communication with other devices). Hence, transmission media can also take the form of waves (including, without limitation, radio, acoustic and/or light waves, such as those generated during radio-wave and infrared data communications).

Common forms of physical and/or tangible computer readable media include, for example, a floppy disk, a flexible disk, a hard disk, magnetic tape, or any other magnetic medium, a CD-ROM, any other optical medium, punch cards, paper tape, any other physical medium with patterns of holes, a RAM, a PROM, an EPROM, a FLASH-EPROM, any other memory chip or cartridge, a carrier wave as described hereinafter, or any other medium from which a computer can read instructions and/or code.

Various forms of computer readable media may be involved in carrying one or more sequences of one or more instructions to the processor(s) **710** for execution. Merely by way of example, the instructions may initially be carried on a magnetic disk and/or optical disc of a remote computer. A remote computer might load the instructions into its dynamic memory and send the instructions as signals over a transmission medium to be received and/or executed by the computer system **700**. These signals, which might be in the form of electromagnetic signals, acoustic signals, optical signals, and/or the like, are all examples of carrier waves on which instructions can be encoded, in accordance with various embodiments of the invention.

The communications subsystem **730** (and/or components thereof) generally will receive the signals, and the bus **705** then might carry the signals (and/or the data, instructions, etc. carried by the signals) to the working memory **735**, from

which the processor(s) **705** retrieves and executes the instructions. The instructions received by the working memory **735** may optionally be stored on a storage device **725** either before or after execution by the processor(s) **710**.

As noted above, a set of embodiments comprises systems collecting presence information and/or enabling remote access to information (including, without limitation, master account information, profiles, and/or videomail) to a user on a user device (in some cases, based on presence information, regardless of whether the user device is owned by and/or associated with the user). FIG. **8** illustrates a schematic diagram of a system **800** that can be used in accordance with one set of embodiments. The system **800** can include one or more user computers **805**. In particular, a user computer **805** can be a video calling device, a PDD, and/or a user device, as described above. More generally, a user computer **805** can be a general purpose personal computer (including, merely by way of example, desktop computers, workstations, tablet computers, laptop computers, handheld computers, mobile phones, smart phones, and the like), running any appropriate operating system, several of which are available from vendors such as Apple, Microsoft Corp., as well as a variety of commercially-available UNIX™ or UNIX-like operating systems. A user computer **805** can also have any of a variety of applications, including one or more applications configured to perform methods provided by various embodiments (as described above, for example), as well as one or more office applications, database client and/or server applications, and/or web browser applications. Alternatively, a user computer **805** can be any other electronic device, such as a thin-client computer, Internet-enabled mobile telephone, and/or personal digital assistant, capable of communicating via a network (e.g., the network **810** described below) and/or of displaying and navigating web pages or other types of electronic documents. Although the exemplary system **800** is shown with two user computers **805**, any number of user computers can be supported.

Certain embodiments operate in a networked environment, which can include a network **810**. The network **810** can be any type of network familiar to those skilled in the art that can support data communications using any of a variety of commercially-available (and/or free or proprietary) protocols, including, without limitation, TCP/IP, SNA™, IPX™, AppleTalk™, and the like. Merely by way of example, the network **810** can include a local area network ("LAN"), including, without limitation, a fiber network, an Ethernet network, a Token-Ring™ network and/or the like; a wide-area network; a wireless wide area network ("WWAN"); a virtual network, such as a virtual private network ("VPN"); the Internet; an intranet; an extranet; a public switched telephone network ("PSTN"); an infra-red network; a wireless network, including without limitation a network operating under any of the IEEE 802.11 suite of protocols, the Bluetooth™ protocol known in the art, and/or any other wireless protocol; and/or any combination of these and/or other networks.

Embodiments can also include one or more server computers **815**. Each of the server computers **815** may be configured with an operating system, including, without limitation, any of those discussed above with respect to the user computers **805**, as well as any commercially (or freely) available server operating systems. Each of the servers **815** may also be running one or more applications, which can be configured to provide services to one or more clients **805** and/or other servers **815**.

Merely by way of example, one of the servers **815** might be a control server, with the functionality described above. In another embodiment, one of the servers might be a web

server, which can be used, merely by way of example, to provide communication between a user computer **805** and a control server, for example, to process requests for web pages or other electronic documents from user computers **805** and/or to provide user input to the control server. The web server can also run a variety of server applications, including HTTP servers, FTP servers, CGI servers, database servers, Java servers, and the like. In some embodiments of the invention, the web server may be configured to serve web pages that can be operated within a web browser on one or more of the user computers **805** to perform operations in accordance with methods provided by various embodiments.

The server computers **815**, in some embodiments, might include one or more application servers, which can be configured with one or more applications accessible by a client running on one or more of the client computers **805** and/or other servers **815**. Merely by way of example, the server(s) **815** can be one or more general purpose computers capable of executing programs or scripts in response to the user computers **805** and/or other servers **815**, including, without limitation, web applications (which might, in some cases, be configured to perform methods provided by various embodiments). Merely by way of example, a web application can be implemented as one or more scripts or programs written in any suitable programming language, such as Java™, C, C#™ or C++, and/or any scripting language, such as Perl, Python, or TCL, as well as combinations of any programming and/or scripting languages. The application server(s) can also include database servers, including, without limitation, those commercially available from Oracle™, Microsoft™, Sybase™, IBM™ and the like, which can process requests from clients (including, depending on the configuration, dedicated database clients, API clients, web browsers, etc.) running on a user computer **805** and/or another server **815**. In some embodiments, an application server can create web pages dynamically for displaying the information in accordance with various embodiments, such as providing a user interface for a control server, as described above. Data provided by an application server may be formatted as one or more web pages (comprising HTML, JavaScript, etc., for example) and/or may be forwarded to a user computer **805** via a web server (as described above, for example). Similarly, a web server might receive web page requests and/or input data from a user computer **805** and/or forward the web page requests and/or input data to an application server. In some cases a web server may be integrated with an application server.

In accordance with further embodiments, one or more servers **815** can function as a file server and/or can include one or more of the files (e.g., application code, data files, etc.) necessary to implement various disclosed methods, incorporated by an application running on a user computer **805** and/or another server **815**. Alternatively, as those skilled in the art will appreciate, a file server can include all necessary files, allowing such an application to be invoked remotely by a user computer **805** and/or server **815**.

It should be noted that the functions described with respect to various servers herein (e.g., application server, database server, web server, file server, etc.) can be performed by a single server and/or a plurality of specialized servers, depending on implementation-specific needs and parameters. Further, as noted above, the functionality of one or more servers **815** might be implemented by one or more containers or virtual machines operating in a cloud environment and/or a distributed, cloud-like environment based on shared resources of a plurality of user video calling devices and/or a plurality of PDDs.

In certain embodiments, the system can include one or more data stores **820**. The nature and location of the data stores **820** is discretionary: merely by way of example, one data store **820** might comprise a database **820a** that stores information about master accounts, user profiles, user preferences, assigned video calling devices, etc. Alternatively and/or additionally, a data store **820b** might be a cloud storage environment for storing master accounts, user profiles, user preferences, uploaded videomail messages, and/or the like. As the skilled reader can appreciate, the database **820a** and the cloud storage environment **820b** might be collocated and/or separate from one another. Some or all of the data stores **820** might reside on a storage medium local to (and/or resident in) a server **815a**. Conversely, any of the data stores **820** (and especially the cloud storage environment **820b**) might be remote from any or all of the computers **805**, **815**, so long as it can be in communication (e.g., via the network **810**) with one or more of these. In a particular set of embodiments, a database **820a** can reside in a storage-area network (“SAN”) familiar to those skilled in the art, and/or the cloud storage environment **820b** might comprise one or more SANs. (Likewise, any necessary files for performing the functions attributed to the computers **805**, **815** can be stored locally on the respective computer and/or remotely, as appropriate.) In one set of embodiments, the database **820a** can be a relational database, such as an Oracle database, that is adapted to store, update, and retrieve data in response to SQL-formatted commands. The database might be controlled and/or maintained by a database server, as described above, for example.

As noted above, the system can also include a first video calling device **825** and a second video calling devices **830**. The first video calling device **825** in the context of the examples described herein corresponds to the device associated with the user or callee, while the second video calling device **830** corresponds to the device associated with the caller. The system might further include a third video calling device **835** from which the user or callee can remotely access the user’s master account, user preferences, videomail, and/or the like. In some embodiments, the third video calling device **835** might be configured to enable presence detection functionalities described in detail above. Although only three video calling devices are illustrated in FIG. **8**, it should be appreciated that any number of video calling devices **825-835** may be implemented in accordance with various embodiments. Using the techniques described herein, the first video calling device **825** or the second video calling device **830** can determine whether or not the user or callee is available for a video call initiated by the second video calling device **830**, prompt the caller to leave a videomail message based at least in part on a determination that the user or callee is not available, record the videomail message, and send the videomail message for post-processing (in some cases, by one of the servers **815**). Each of the first video calling devices **825**, the second video calling devices **830**, and/or the third video calling devices **835** may be (or may have similar functionality as) a video calling device **105** or a PDD **105**, as described in detail above; in some cases, each of the first video calling devices **825**, the second video calling devices **830**, and/or the third video calling devices **835** might be (or may have similar functionality as) a VCD as described in the ‘182 patent.

While certain features and aspects have been described with respect to exemplary embodiments, one skilled in the art will recognize that numerous modifications are possible. For example, the methods and processes described herein may be implemented using hardware components, software components, and/or any combination thereof. Further, while various methods and processes described herein may be described

with respect to particular structural and/or functional components for ease of description, methods provided by various embodiments are not limited to any particular structural and/or functional architecture but instead can be implemented on any suitable hardware, firmware, and/or software configuration. Similarly, while certain functionality is ascribed to certain system components, unless the context dictates otherwise, this functionality can be distributed among various other system components in accordance with the several embodiments.

Moreover, while the procedures of the methods and processes described herein are described in a particular order for ease of description, unless the context dictates otherwise, various procedures may be reordered, added, and/or omitted in accordance with various embodiments. Moreover, the procedures described with respect to one method or process may be incorporated within other described methods or processes; likewise, system components described according to a particular structural architecture and/or with respect to one system may be organized in alternative structural architectures and/or incorporated within other described systems. Hence, while various embodiments are described with—or without—certain features for ease of description and to illustrate exemplary aspects of those embodiments, the various components and/or features described herein with respect to a particular embodiment can be substituted, added, and/or subtracted from among other described embodiments, unless the context dictates otherwise. Consequently, although several exemplary embodiments are described above, it will be appreciated that the invention is intended to cover all modifications and equivalents within the scope of the following claims.

What is claimed is:

1. A method, comprising:

receiving, at a first video calling device associated with a user and over a network, a video call from a caller at a second video calling device;

determining, with one or both of the first video calling device or the second video calling device, that the user is unable to answer the video call;

recording, with the first video calling device that receives the call, a videomail message from the video call, based at least in part on a determination that the user is unable to answer the video call;

uploading, with the first video calling device, the videomail message to a server over the network;

post-processing, with the server, at least a portion of the videomail message that has been uploaded over the network, wherein post-processing comprises scaling video of the videomail message being of a first resolution and scaling video of second videomail messages from third video calling devices being of a second resolution all to a single consistent specified resolution;

providing, with the first video calling device, user access to a web portal interface running on the server, the web portal interface providing the user with access to the videomail message that has been post-processed to be of the single consistent specified resolution and that is viewable through the web portal interface;

creating a uniform resource locator (“URL”) addressing the videomail message that has been post-processed to be of the single consistent specified resolution; and

providing a notification to the user, the notification containing the URL addressing the videomail message that has been post-processed to be of the single consistent specified resolution.

51

2. The method of claim 1, wherein the first video calling device and the second video calling device are at least one of made by different manufacturers or of different models of calling device.

3. The method of claim 1, further comprising:
prompting, with the first video calling device associated with the user, the caller to leave the videomail message.

4. The method of claim 1, wherein each of at least one of the first video calling device or the second video calling device comprises:

a first video input interface to receive first video input from a first local content source;

a first audio input interface to receive first audio input from the first local content source;

a first video output interface to provide first video output to a first video display device;

a first audio output interface to provide first audio output to a first audio receiver;

a first video capture device to capture at least one of first image data or first video data;

a first audio capture device to capture first audio data;

a first network interface;

at least one first processor; and

a first storage medium in communication with the at least one first processor.

5. The method of claim 1, wherein uploading the videomail message to the server over the network comprises uploading at least a portion of each of one or more components of the videomail message, the one or more components of the videomail message comprising an audio component, a video component, and a timecode component.

6. The method of claim 1, wherein post-processing further comprises mixing audio and video of the videomail message by reference to a timecode.

7. The method of claim 1, wherein post-processing further comprises adding a visible watermark to the videomail message.

8. The method of claim 1, wherein post-processing further comprises formatting the videomail message as a video viewable by a web browser that accesses the web portal interface.

9. The method of claim 1, wherein post-processing further comprises formatting the videomail message for downloading by the user.

10. The method of claim 1, wherein post-processing further comprises formatting the videomail message for viewing on a user device.

11. The method of claim 1, further comprising:

recording a timecode file to a storage medium at one of the first video calling device, the second video calling device, or the server, the timecode file indicating when each frame of video of the videomail message should be displayed and indicating when each frame of audio of the videomail message should be played;

synchronizing, at the one of the first video calling device, the second video calling device, or the server, audio and video from the videomail message, based at least in part on the recorded timecode file;

wherein uploading the videomail message to the server comprises uploading an audio file, a video file, and the timecode to the server.

12. The method of claim 1, wherein the notification further comprises an e-mail message, in which the videomail message is one of an attached videomail message or an embedded videomail message.

13. The method of claim 1, wherein the notification further comprises a text message with a link to a formatted video comprising the videomail message.

52

14. The method of claim 1, wherein the notification further comprises an e-mail message with a link to a formatted video comprising the videomail message.

15. The method of claim 14, further comprising:

creating a second uniform resource locator ("URL") addressing the formatted video, wherein the link includes the second URL addressing the formatted video.

16. The method of claim 1, further comprising:

registering, with a first computer, a master account for the user;

assigning, with the first computer, the first video calling device to the master account;

authenticating the user, at the first computer, using a set of credentials associated with the master account;

accessing the first video calling device from the first computer, over the network, after authenticating the user;

providing a user interface, from the first computer, over the network;

receiving, by the first computer, user input associated with options presented by the user interface, the options including one or more of options for establishing user preferences for videomail messages, options for modifying user preferences for videomail messages, options for deleting user preferences for videomail messages, options for notifying the user regarding videomail messages, or options for responding to videomail messages.

17. The method of claim 16, wherein the network is the Internet, and wherein the user interface comprises a web page.

18. The method of claim 16, further comprising:

receiving a request from the user to view the videomail message; and

displaying the videomail message with the user interface.

19. The method of claim 16, wherein the first computer is one of the first video calling device or the second video calling device.

20. The method of claim 16, wherein receiving user input comprises receiving user input from a third video calling device, the third video calling device comprising:

a second video input interface to receive second video input from a second local content source;

a second audio input interface to receive second audio input from the second local content source;

a second video output interface to provide second video output to a second video display device;

a second audio output interface to provide second audio output to a second audio receiver;

a second video capture device to capture at least one of second image data or second video data;

a second audio capture device to capture second audio data;

a second network interface;

at least one second processor; and

a second storage medium in communication with the at least one second processor;

the method further comprising:

providing the user with access, over the network, to at least one of the first video calling device or the master account.

21. The method of claim 20, further comprising:

collecting presence information with the third video calling device;

detecting presence of the user, with the third video calling device, based at least in part on the presence information;

53

identifying the user, with a second computer, based at least in part on identifying information derived from at least a portion of the presence information; and
in response to identifying the user, providing, over the third video calling device, options for the user to view any videomail messages left for the user.

22. The method of claim 21, wherein identifying the user comprises one or more of:

- analyzing, with the second computer, at least one of captured second image data or captured second video data, using facial recognition software;
- comparing, with the second computer, at least a portion of the captured second audio data with a voiceprint;
- comparing, with the second computer, at least a portion of the captured second audio data with stored challenge/response information;
- determining, with the second computer, whether a username and a password inputted by the user matches a pre-stored username and a pre-stored password associated with the user;
- determining, with the second computer, whether a user device that is detected in proximity to the presence detection device is a device associated with the user; or
- detecting a presence of a user device that is associated with the user, based on at least one of detecting a Bluetooth connection of the user device, detecting that the user device is associated with a WiFi access point with which the presence detection device has associated, or communicating with the user device using near field communication ("NFC").

23. An apparatus, comprising:

- one or more processors; and
- a computer readable medium in communication with the one or more processors, the computer readable medium having encoded thereon a set of instructions executable by the one or more processors to cause the apparatus to perform one or more operations, the set of instructions comprising:
 - instructions for receiving a video call from a video calling device;
 - instructions for determining that the user is unable to answer the video call;
 - instructions for recording a videomail message from the video call, based at least in part on a determination that the user is unable to answer the video call;
 - instructions for uploading the videomail message to a server over the network;
 - instructions for post-processing, with the server, at least a portion of the videomail message that has been uploaded over the network, wherein post-processing comprises scaling video of the videomail message being of a first resolution and scaling video of second videomail messages from third video calling devices being of a second resolution all to a single consistent specified resolution;
 - instructions for providing user access to a web portal interface running on the server, the web portal interface providing the user with access to the videomail message that has been post-processed to be of the single consistent specified resolution and that is viewable through the web portal interface; and
 - instructions for providing a notification to the user, the notification containing a uniform resource locator ("URL") that has been created to address the videomail message that has been post-processed to be of the single consistent specified resolution.

54

24. A video calling device, comprising:

- one or more processors; and
- a computer readable medium in communication with the one or more processors, the computer readable medium having encoded thereon a set of instructions executable by the one or more processors to cause the video calling device to perform one or more operations, the set of instructions comprising:
 - instructions for sending a video call to an apparatus;
 - instructions for determining that a callee associated with the apparatus is not available to answer the video call;
 - instructions for recording a videomail message from the video call, based at least in part on a determination that the callee is unable to answer the video call;
 - instructions for uploading the videomail message to a server over a network;
 - instructions for post-processing, with the server, at least a portion of the videomail message that has been uploaded over the network, wherein post-processing comprises scaling video of the videomail message being of a first resolution and scaling video of second videomail messages from third video calling devices being of a second resolution all to a single consistent specified resolution
 - instructions for sending a first notification to the callee with instructions to access the videomail message via a web portal interface running on the server, the web portal interface providing the callee with access to the videomail message that has been post-processed to be of the single consistent specified resolution and that is viewable through the web portal interface; and
 - instructions for providing a notification to the user, the notification containing a uniform resource locator ("URL") that has been created to address the videomail message that has been post-processed to be of the single consistent specified resolution.

25. A system, comprising:

- a first video calling device associated with a user, the first video calling device comprising:
 - one or more first processors; and
 - a first computer readable medium in communication with the one or more first processors, the first computer readable medium having encoded thereon a first set of instructions executable by the one or more first processors to cause the first video calling device to perform one or more operations, the first set of instructions comprising:
 - instructions for receiving a video call from a caller at a second video calling device;
 - instructions for determining that the user is unable to answer the video call;
 - instructions for recording a videomail message from the video call, based at least in part on a determination that the user is unable to answer the video call;
 - instructions for uploading the videomail message to a server over the network; and
 - instructions for providing user access to a web portal interface running on the server, the web portal interface providing the user with access to the videomail message that is viewable through the web portal interface; and
- a server computer, comprising:
 - one or more second processors; and
 - a second computer readable medium in communication with the one or more second processors, the second computer readable medium having encoded thereon a

second set of instructions executable by the one or more second processors to cause the server computer to perform one or more operations, the second set of instructions comprising:

instructions for receiving the uploaded videomail 5 message;

instructions for post-processing, with the server, at least a portion of the videomail message that has been uploaded over the network, wherein post-processing comprises scaling video of the videomail 10 message being of a first resolution and scaling video of second videomail messages from third video calling devices being of a second resolution all to a single consistent specified resolution;

instructions for establishing or maintaining the web 15 portal interface;

instructions for creating a uniform resource locator ("URL") addressing the videomail message that has been post-processed to be of the single consistent specified resolution; and 20

instructions for providing a notification to the user, the notification containing the URL addressing the videomail message that has been post-processed to be of the single consistent specified resolution. 25

* * * * *